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

| | |
|---|---|
| In re: Arby's Restaurant Group, Inc. Data Security Litigation<br><br>CONSOLIDATED CONSUMER CASE | Case No. 1:17-cv-1035-AT |

# CONSUMER PLAINTIFFS' FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Jacqueline Weiss, Joseph Weiss, Ashley Russell, Brett Barnes and Burnell Rutters (hereinafter, collectively, "Consumer Plaintiffs"), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Arby's Restaurant Group, Inc. ("ARG") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

## NATURE OF THE CASE

1. Consumer Plaintiffs bring this class action case against Defendant ARG for its failures to secure and safeguard Arby's customers' credit and debit card numbers and other payment card data ("PCD"), and other personally identifiable information ("PII") which ARG collected at the time Consumer

Plaintiffs made purchases at Arby's restaurants owned and operated by ARG, and for failing to provide timely, accurate and adequate notice to Consumer Plaintiff and other Class members that their PCD and PII (hereinafter, collectively, "Customer Data") had been stolen and precisely what types of information were stolen.

2. ARG has acknowledged that customers who used payment cards for transactions at approximately 1,000 Arby's corporate-owned restaurants located throughout the United States had their Customer Data stolen starting in or around October 2016 and continuing through January 12, 2017.

3. In or around October 2016, computer hackers began using malicious software, known as "malware," to access the point-of-sale ("POS") systems at Arby's locations to gain access to Customer Data, including credit and debit card numbers (the "Data Breach").

4. This private Customer Data was compromised due to ARG's acts and omissions and their failure to properly protect the Customer Data.

5. ARG could have prevented this Data Breach. Data breaches at other restaurant chains and retail establishments in the last few years have been the result of malware installed on POS systems. While many retailers, restaurant chains and

other companies have responded to recent breaches by adopting technology that helps make transactions more secure, ARG did not.

6. In addition to ARG's failure to prevent the Data Breach, ARG also failed to detect the breach for nearly three months, and only learned of it after "industry partners" notified ARG of the breach in mid-January 2017.

7. When ARG finally learned of the breach in January 2017, however, it made no immediate public announcement and provided no information to its customers. Only after Brian Krebs, a data security investigator, reported on his blog, KrebsOnSecurity.com, that ARG had suffered a data breach via malware placed on Arby's restaurants' POS systems did ARG finally acknowledge that Customer Data had been compromised as a result of its systems being breached.[1]

8. Finally, in April 2017, nearly three months after the Data Breach supposedly ended, and six months after it began, ARG disclosed the extent of its massive data breach: over 950 restaurants were infected with malware for an average of 73 days, with some restaurants infected for more than three months. Some financial institutions have reported that more payment cards were compromised in the Arby's Data Breach than in any other single breach.

[1] Brian Krebs, *Fast Food Chain Arby's Acknowledges Breach*, KrebsOnSecurity (Feb. 17, 2017), https://krebsonsecurity.com/2017/02/fast-food-chain-arbysacknowledges-breach/ (last visited July 18, 2017).

9. The Data Breach was the inevitable result of ARG's inadequate approach to data security and the protection of the Customer Data that it collected during the course of its business. The deficiencies in ARG's data security were so significant that the malware installed by the hackers remained undetected and intact for months.

10. The susceptibility of POS systems to malware is well-known throughout the restaurant industry, as well as the retail industry. In the last five years, practically every major data breach involving retail stores or fast-food restaurant chains has been the result of malware placed on POS systems. Accordingly, data security experts have warned companies, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[2] Unfortunately, ARG's profit-driven decisions to ignore these warning led to the damage upon which this case is based.

11. The threat of a breach of POS systems was, or should have been, well known to ARG. From October 2015 until June 2016, over 1,000 Wendy's — restaurants also owned by the parent company of ARG — were breached as a

[2] Datacap Systems Inc., *Point of sale security: Retail data breaches at a glance*, https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance# (last visited July 17, 2017).

result of hackers deploying malware across POS systems to extract payment card information.[3]

12. ARG disregarded the rights of Consumer Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard Customer Data, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

13. In addition, ARG exacerbated the injuries suffered by Consumer Plaintiffs and the Class by failing to provide timely notice of the infiltration when it supposedly learned of the breach in January. If ARG had promptly notified the public of the Data Breach, the resulting losses would have been less significant.

14. As a result of the Arby's Data Breach, the Customer Data of the Consumer Plaintiffs and Class members has been exposed to criminals for misuse. The injuries suffered by Consumer Plaintiffs and Class members as a direct result of the Arby's Data Breach include:

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

[3] Krebs, *supra* note 1.

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their debit or credit card accounts because their account were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Arby's Data Breach, including but not limited to foregoing cash back rewards;

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

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on

compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Arby's Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Consumer Plaintiffs' and Class members' information on the Internet black market;

h. money paid for products and services purchased at ARG stores during the period of the Arby's Data Breach, in that Consumer Plaintiffs and Class members would not have dined at Arby's had ARG disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Customer Data;

i. damages to and diminution in value of their Customer Data entrusted to ARG for the sole purpose of purchasing products and services from ARG; and

j. the loss of Consumer Plaintiffs and Class members' privacy.

15. The injuries to the Consumer Plaintiffs and Class members were directly and proximately caused by ARG's failure to implement or maintain adequate data security measures for Customer Data.

16. Further, Consumer Plaintiffs retain a significant interest in ensuring that their Customer Data, which, while stolen, remains in the possession of ARG is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose Customer Data was stolen as a result of the Arby's Data Breach.

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

## JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from ARG.

19. This Court has personal jurisdiction over ARG because ARG 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 marketing and selling products and services and by accepting and processing payments for those products and services within Georgia.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because ARG's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

## PARTIES

21. Plaintiffs Jacqueline Weiss and Joseph Weiss are residents of the state of Connecticut.

22. Plaintiff Ashley Russell is a resident of the state of Tennessee.

23. Plaintiff Brett Barnes is a resident of the state of Georgia.

24. Plaintiff Burnell Rutters is a resident of the state of Florida.

25. Defendant Arby's Restaurant Group, Inc. is a Delaware corporation with its principal place of business located at 1155 Perimeter Center, Suite 1200, Atlanta, Georgia 30338. ARG is owned by Roark Capital Group and Wendy's Company.

26. ARG's restaurant system consists of over 3,300 corporate-owned and franchisee-owned locations across the U.S. and worldwide. Approximately one third of these are corporate-owned restaurants, which are the focus of this matter.

27. ARG restaurants accept payment for goods and services through a point of sale system ("POS system"), through which customers swipe credit and debit cards to pay.

## STATEMENT OF FACTS

### A. Consumer Plaintiffs' Transactions

28. On or around November 20, 2016, Plaintiffs Jacqueline and Joseph Weiss purchased food at an Arby's restaurant located at 3206 Berlin Turnpike, Newington, Connecticut using a jointly held Fidelity Visa credit card.

29. ARG has confirmed that the location visited by Plaintiffs Jacqueline Weiss and Joseph Weiss was affected by the Data Breach.[4]

30. In or around December 2016, Mr. and Mrs. Weiss discovered thousands of dollars in unauthorized charges on the Fidelity Visa credit card, and were forced to cancel that credit card as a result. This compromise of the Fidelity Visa credit card occurred even though Mr. and Mrs. Weiss had physical possession of the payment card at all times. Plaintiffs Jacqueline Weiss and Joseph Weiss were required to expend time contacting the credit card company and attempting to resolve the issues caused by the theft of their identity. During the period of time they were awaiting their replacement card, Plaintiffs Jacqueline Weiss and Joseph

[4] List of affected Arby's restaurant locations, available at: http://arbys.com/security/ (last visited July 17, 2017).

Weiss had to use alternative sources of funds to make purchases, thereby foregoing rewards points and/or cash-back rewards they accrue with use of the Fidelity Visa credit card.

31. Plaintiffs Jacqueline Weiss and Joseph Weiss suffered actual injury from having their Customer Data compromised and stolen in and as a result of the Arby's Data Breach.

32. On or around December 3, 2016, Plaintiff Ashley Russell visited an Arby's restaurant located at 601 Old Hickory Road in Jackson, Tennessee and purchased food using her debit card issued by her bank.

33. ARG has confirmed that the location visited by Plaintiff Ashley Russell was affected by the Data Breach.[5]

34. Within a few months after December 3, 2016, Ms. Russell was contacted by her bank and advised that her card had been compromised. This compromise of Ms. Russell's debit card occurred even though she had physical possession of her payment card at all times. The bank informed Ms. Russell that it was cancelling her debit card and would issue her a new one. Ms. Russell was not able to withdraw money before the bank cancelled her card. Ms. Russell had to travel out-of-state and because she did not have cash or an active debit card to use,

[5] *Id.*

she did not have sufficient funds to pay for her expenses. Ms. Russell was without a debit card for approximately ten days before she received a new card from her bank. As a result of the Data Breach, Ms. Russell was required to spend time communicating with her bank regarding her compromised card, the cancellation of her card and the issuing of a replacement card.

35. Plaintiff Ashley Russell suffered actual injury from having her Customer Data compromised and stolen in and as a result of the Arby's Data Breach.

36. On or around November 16, 2016, Plaintiff Brett Barnes purchased food at an Arby's restaurant located at 5410 Peachtree Industrial Blvd, Chamblee, Georgia 30341, using a United Bank Visa credit card.

37. ARG has confirmed that the location visited by Plaintiff Barnes was affected by the Data Breach.[6]

38. On or around March 18, 2017, Mr. Barnes was contacted by United Bank Visa to report 28 transactions of suspicious account activity, totaling $1,579.64 and occurring in rapid succession over the course of the previous four (4) days in areas of the state where Mr. Barnes does not typically shop. When Mr. Barnes verified the charges were unauthorized, the United Bank Visa

[6] *Id.*

representative told Mr. Barnes that the bank noticed he has made a purchase at an Arby's in Chamblee, Georgia, on November 16, 2017, and that the compromise of his card probably originated from the Arby's Data Breach. Mr. Barnes' credit card was cancelled and a replacement card was sent a few days later.

39. The compromise of Mr. Barnes' United Bank Visa credit card occurred even though he had physical possession of the payment card at all times. Plaintiff Barnes was required to expend time communicating with the credit card company and attempting to resolve the issues caused by the theft of his identity. During the period of time he was awaiting a replacement card, Mr. Barnes had to use alternative sources of funds to make purchases, thereby foregoing rewards points and/or cash-back rewards they accrue with use of the United Bank Visa credit card.

40. Plaintiff Brett Barnes suffered actual injury from having his Customer Data compromised and stolen in and as a result of the Arby's Data Breach.

41. On October 27, 2016 and January 14, 2017, Plaintiff Burnell Rutters made food purchases at an Arby's restaurant located at 2600 S. Orange Ave, Orlando, FL 32806, using his McCoy Federal Credit Union debit card.

42. ARG has confirmed that the location visited by Plaintiff Rutters was affected by the Data Breach.[7]

43. Shortly after making the January 14, 2017 purchase at Arby's, Plaintiff Rutters attempted to use his debit card for a purchase and it was declined. When he contacted McCoy Federal Credit Union, he was informed that his debit card had been compromised in a data breach, that there was suspicious activity on his account and that his debit card had been cancelled without any notice to him. Due to various problems with continued fraudulent charges on his bank account and failed reactivation of three new debit cards, Plaintiff Rutters was prevented from using his debit card for approximately two months. Purchases were repeatedly declined when he attempted to use the debit card for credit transactions and Mr. Rutters had to borrow money from friends to complete his attempted purchases, which caused great annoyance and embarrassment when he had to explain why the purchase was declined.

44. As an additional result of the compromise of his debit card, Plaintiff Rutters was forced to physically go into his bank to withdraw cash on multiple occasions so that he could meet financial obligations and expenses. As Plaintiff Rutters' bank was not open after 5pm, or on weekends, he had to take time off

[7] *Id.*

from work to physically go to the bank to withdraw cash during the normal hours of operation, which caused great inconvenience and hassle.

45. The compromise of Mr. Rutters' McCoy Federal Credit Union debit card occurred even though he had physical possession of the payment card at all times. Plaintiff Rutters has been forced to expend significant time communication with bank representatives and monitoring his bank statements for fraudulent and unauthorized charges, and will continue to expend significant time to determine whether his personal information was compromised in the Arby's data breach.

46. Plaintiff Burnell Rutters suffered actual injury from having his Customer Data compromised and stolen in and as a result of the Arby's Data Breach.

47. Consumer Plaintiffs would not have used their payment cards to make purchases at ARG had ARG told them that it lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft. Indeed, Consumer Plaintiffs would not have shopped at Arby's at all during the period of the Arby's Data Breach and, thus, they suffered actual injury and damages in paying money to for the purchase of products from ARG that they would not have paid had ARG made such disclosure.

48. Consumer Plaintiffs also suffered actual injury in the form of damages to and diminution in the value of their Customer Data – a form of intangible property that Consumer Plaintiffs entrusted to ARG for the purpose of purchasing its products and that was compromised in and as a result of the Arby's Data Breach.

49. Additionally, Consumer Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their Customer Data being placed in the hands of criminals who have already misused such information, as evidenced by the compromise of Consumer Plaintiffs' payment cards.

50. Moreover, Consumer Plaintiffs have a continuing interest in ensuring that their private information, which remains in the possession of ARG, is protected and safeguarded from future breaches.

**B. ARG and Its Customer Data Collection Practices**

51. In 2016, ARG produced system-wide sales of more than $3.6 billion.

52. ARG operates Arby's restaurants, a fast-food restaurant chain specializing in roast beef and other protein-based sandwiches. The first Arby's restaurant opened in 1964 and, since then, Arby's has expanded to nearly 3,300 restaurants worldwide, including approximately 1,000 restaurants owned and

operated by ARG (those at issue in this Data Breach) and the remainder operating under a franchisee license agreement.

53. In 2016, ARG produced system-wide sales of more than $3.6 billion.

54. With its growing profitability, ARG has heavily invested in remodeling its restaurants. In 2014, ARG launched its "Inspire Design" restaurant, a remodeling effort which ARG claims has boosted sales by 15% at remodeled restaurants.[8] 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.[9]

55. Despite ARG's substantial investments made to modernize its branding and upgrade the appearance of its restaurants, ARG failed to make meaningful improvements to the security of its POS systems and administrative network, placing the purchasing information of its customers at risk [10]

---

[8] *Brand Milestones*, Arbys.com, http://arbysfranchising.com/research/brand-milestones/ (last visited July 18, 2017).

[9] Beth Kowitt, *How Arby's (Yes, Arby's) Is Crushing It*, Fortune (Apr. 27, 2016), available at: http://fortune.com/2016/04/27/arbys-sales-growth/ (last visited July 18, 2017).

[10] On information and belief, ARG contracted with various third parties to install, manage, service and maintain the POS equipment and software who may also be responsible or liable for allowing the hackers to gain access and deploy malware on the POS systems in ARG's network. Consumer Plaintiffs hereby provide Notice that after discovery, they may seek leave to add those third party vendors as party defendants in this litigation.

56. A significant portion of sales at ARG are made using credit or debit cards. When customers pay using credit or debit cards, ARG collects Customer Data related to those cards including the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. ARG stores the Customer Data in its POS system and transmits this information to a third party for processing and completion of the payment.

57. At all relevant times, ARG was well-aware, or reasonably should have been aware, that the Customer Data collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

58. It is well known and the subject of many media reports that Customer Data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches by retailers and restaurant chains, ARG maintained an insufficient and inadequate system to protect the Customer Data of Consumer Plaintiffs and Class members.

59. Customer Data is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, social security numbers, and

other personal information on a number of underground Internet websites. Customer Data is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

60. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[11]

61. At all relevant times, ARG knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

62. ARG was, or should have been, fully aware of the significant volume of daily credit and debit card transactions at Arby's restaurants, amounting to tens

[11] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 10, 2017).

of thousands of daily payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of ARG's systems.

63. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of Customer Data in the hands of other third parties, such as retailers and fast-food restaurant chains, ARG's approach to maintaining the privacy and security of the Customer Data of Consumer Plaintiffs and Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

**C. ARG Had Notice of Data Breaches Involving Malware on POS Systems**

64. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[12] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[13] The amount of payment card data compromised by data breaches is massive. For example, it is estimated that over 100 million cards were compromised in 2013 and 2014.[14]

---

[12] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, Identity Theft Resource Center (Jan. 19, 2017), http://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208 (last visited July 17, 2017).

[13] *Id.*

[14] Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20,

65. Most of the massive data breaches occurring within the last several years involved malware placed on POS systems used by merchants. A POS system is an on-site device, much like an electronic cash register, which manages transactions from consumer purchases, both by cash and card. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."[15] The payment processor then passes on the payment information to the financial institution that issued the card and takes the other steps needed to complete the transaction.[16]

66. Before transmitting customer data over the merchant's network, POS systems typically, and very briefly, store the data in plain text within the system's memory.[17] The stored information includes "Track 1" and "Track 2" data from the magnetic strip on the payment card, such as the cardholder's first and last name, the

---

2014), available at: https://origin-www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf (last visited July 17, 2017).

[15] Symantec, *supra* note 13, at 6.

[16] Salva Gomzin, *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions*, 8 (Wiley 2014), *available at:* http://1.droppdf.com/files/IS0md/wiley-hacking-point-of-sale-payment-application-secrets-threats-and-solutions-2014.pdf (last visited July 18, 2017).

[17] *Id.* at 39.

expiration date of the card, and the CVV (three number security code on the card).[18] This information is unencrypted on the card and, at least briefly, will be unencrypted in the POS terminal's temporary memory as it processes the data. [19]

67. In ordered to directly access a POS device, hackers generally follow four steps: infiltration, propagation, exfiltration and aggregation.[20] In the infiltration phase, an "attacker gains access to the target environment"[21] allowing the hackers to move through a business's computer network, find an entry point into the area that handles consumer payments, and directly access the physical POS machines at in-store locations.[22] Once inside the system the attacker then infects the POS systems with malware, which "collects the desired information . . . and then exfiltrates the data to another system" called the "aggregation point."[23]

68. A 2016 report by Verizon confirmed "[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

---

[18] *Id*. at 43-50.
[19] Symantec, *supra* note 13, at 5.
[20] *Point of Sale Systems and Security: Executive Summary*, SANS Institute, 4 (Oct. 2014), available at: https://www.sans.org/reading-room/whitepapers/analyst/point-salesystems-security-executive-summary-35622 (last visited July 18, 2017).
[21] *Id*.
[22] Symantec, *supra* note 13, at 6.
[23] *Id*.

RAM scraper, to capture payment card data."[24] According to Verizon, hackers successfully compromise POS systems in a matter of minutes or hours and exfiltrate data within days of placing malware on the POS devices.[25]

69. Intruders with access to unencrypted Track 1 and Track 2 payment card data can physically replicate the card or use it online. Unsurprisingly, theft of payment card information via POS systems is now "one of the biggest sources of stolen payment cards."[26] Since 2014, malware installed on POS systems has been responsible for nearly every major data breach of a retail outlet or restaurant.[27] In 2015, intrusions into POS systems accounted for 64% of all breaches where intruders successfully stole data.[28] For example, in 2013, hackers infiltrated Target, Inc.'s POS system, stealing information from an estimated 40 million payment cards in the United States.[29] In 2014, over 7,500 self-checkout POS terminals at Home Depots throughout the United States were hacked, compromising roughly 56 million debit and credit cards.[30]

---

[24] *Id*.
[25] *Id*. at 4.
[26] Symantec, *supra* note 13, at 3.
[27] See, e.g., *2016 Data Breach Investigations Report*, Verizon, at 1 (Apr. 2016), http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Retail-DataSecurity_en_xg.pdf. (last visited July 18, 2017).
[28] *Id*. at 3.
[29] Krebs, *supra* note 1.
[30] Brett Hawkins, *Case Study: The Home Depot Data Breach*, 7 (SANS Institute,

70. As mentioned above, POS systems at more than 1,000 Wendy's restaurants were infiltrated with malware, resulting in the theft of payment cards data for approximately six-months.[31] The POS systems data breach at Wendy's should have been a major red flag for ARG, not only because Wendy's operates a similar fast food chain to Arby's but also because between 2008 and 2011, Arby's and Wendy's restaurants were corporate affiliates through a merger, which created the Wendy's/Arby's Group, Inc. Today, the Wendy's Company still maintains an ownership interest in ARG. Further, upon information and belief, ARG's POS systems were operating with the same software compromised in the Wendy's data breach.

71. Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, ARG was well aware or should have been aware of the need to safeguard its POS systems.

**D. ARG Failed to Comply with Industry Standards**

72. Despite the vulnerabilities of POS systems, available security measures and reasonable businesses practices would have significantly reduced or eliminated the likelihood that hackers could successfully infiltrate business' POS

---

Jan. 2015), available at: https://www.sans.org/reading-room/whitepapers/casestudies/casestudy-home-depot-data-breach-36367 (last visited July 18, 2017).

[31] Krebs, *supra* note 1.

systems. One report indicated that over 90% of the data breaches occurring in 2014 were preventable.[32]

73. The payment card networks (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 prevent these types of intrusions into POS systems. However, despite ARG's understanding of the risk of data theft via malware installed on POS systems, the widely available resources to prevent intrusion into POS data systems, and the close experience of the POS systems at Wendy's being hacked, ARG failed to adhere to these guidelines and failed to take reasonable and sufficient protective measures to prevent the Data Breach.

74. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, more than two years ago, Symantec recommended "point to point encryption" implemented through secure card readers, which encrypts credit card information in the POS system, preventing malware that extracts card information through the POS memory while it processes the transaction.[33] Moreover, Symantec emphasized the importance of adopting EMV

[32] Verizon, *supra* note 26, at 1.
[33] Symantec, *supra* note 13, at 6.

chip technology. Last year, Datacap Systems, a developer of POS systems, recommended similar preventative measures.[34]

75. The major payment card industry brands set forth specific 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.

76. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.[35]

77. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[36] PCI DSS sets the minimum level of what must be done, not the maximum.

---

[34] *See* Datacap Systems, *supra* note 2.
[35] *Payment Card Industry Data Security Standard* v3.2, at 5 (April 2016) available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited July 21, 2017.
[36] *Id*.

78. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, impose the following mandates on ARG: [37]

**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<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | 3. Protect stored cardholder data<br>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<br>6. Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | 7. Restrict access to cardholder data by business need to know<br>8. Identify and authenticate access to system components<br>9. Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | 10. Track and monitor all access to network resources and cardholder data<br>11. Regularly test security systems and processes |
| **Maintain an Information Security Policy** | 12. Maintain a policy that addresses information security for all personnel |

79. Among other things, PCI DSS required ARG to properly secure and protect 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; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

80. PCI DSS also required ARG to not store "the full contents of…the magnetic stripe located on the back of a card" or "the card verification code or value" after authorization.[38]

[37] *Id.*

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

**E. ARG Failed to Upgrade its Payment Systems to Use EMV Technology**

82. The payment card industry also sets rules requiring all businesses to upgrade to new card readers that accept EMV chips. Data Security advisors, like Symantec and DataCap Systems, have also strongly encouraged the use of POS terminals capable of accepting payment from EMV chips.

83. EMV chip technology uses embedded computer chips instead of magnetic stripes to store PCD. The magnetic stripe on the back of a debit or credit card contains a code that is recovered by sliding the card through a magnetic stripe reader. The code never changes. Unlike magnetic stripe technology, in which the card information never changes, EMV technology creates a unique transaction code every time the chip is used. Such technology increases payment card security

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

because the unique transaction code cannot be used again, making it more difficult for criminals to use stolen EMV chip card information.

84. The payment card industry, including Visa, MasterCard, and American Express, set a deadline of October 1, 2015 for businesses to transition their POS systems from magnetic stripe readers to readers using EMV chip technology.

85. Upon information and belief, ARG failed to meet the October 1, 2015 deadline for installing EMV chip readers at its restaurants.

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

**F. ARG Failed to Comply With FTC Requirements**

87. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the 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. According to the FTC, the need for data security should be factored into all business decision-making.[39]

[39] Federal Trade Commission, *Start With Security*, available at

88. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[40] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

89. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and

---

https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 10, 2017).

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

verify that third-party service providers have implemented reasonable security measures.[41]

90. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating 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 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. ARG's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

92. In this case, ARG was at all times fully aware of its obligation to protect the financial data of ARG's customers because of its participation in payment card processing networks. ARG was also aware of the significant repercussions if it failed to do so because ARG collected payment card data from tens of thousands of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Consumer Plaintiffs and Class members.

[41] FTC, *Start With Security*, *supra* note 38.

93. Despite understanding the consequences of inadequate data security, ARG failed to comply with PCI DSS requirements; failed to take additional protective measures beyond those required by PCI DSS; and, failed to implement EMV-capable POS systems by the October 1, 2015 deadline;

94. Despite understanding the consequences of inadequate data security, ARG operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take other measures necessary to protect its data network.

## G. The Arby's Data Breach

95. As early as 2009, the predecessor entity of ARG was well-aware of the risks of a data breach:

> We rely on computer systems and information technology to run our business. Any material failure, interruption or security breach of our computer systems or information technology may adversely affect the operation of our business and results of operations.
> We are significantly dependent upon our computer systems and information technology to properly conduct our business. A failure or interruption of computer systems or information technology could result in the loss of data, business interruptions or delays in business operations. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. Any security breach of our computer systems or information technology may result in adverse

> publicity, loss of sales and profits, penalties or loss resulting from misappropriation of information.

ARG/Arby's Restaurants, LLC, Prospectus (Nov. 9, 2009)

96. Further, in the years following this acknowledgment of the risks, massive data breaches plagued the restaurant industry, including national restaurant chains such as Popeye's, Noodles & Co., and P.F. Chang's. Based on the data breaches within the restaurant industry, particularly the significant breach at Wendy's, and ARG's own acknowledgment of the risks as stated above, ARG knew or should have known that its systems were at risk for a similar malware data breach.

97. In or around October 8, 2016, hackers gained access to ARG's data network and installed malware on POS systems at approximately 1,000 ARG corporate-owned restaurant locations nationwide.[42] The malware allowed the thieves to download and steal copies of ARG customers' Customer Data until at least January 12, 2017.

98. PSCU, a credit union organization that serves 800 credit unions, was the first to report the breach, reporting that both Track 1 and Track 2 data may have been compromised in the Arby's data breach. Track 1 and Track 2 data normally includes credit and debit card information such as the cardholder name,

[42] http://arbys.com/security/ (last visited on April 10, 2017).

primary account number, expiration date, and, in certain instances, PIN number. The PSCU alert also estimated that the "exposure window" was a three-month time period between October 2016 and January 2017.[43]

99. The breach became public on February 9, 2017 through an article published by Brian Krebs of KrebsOnSecruity, not by any announcement from ARG.[44]

100. 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] Krebs, *supra* note 1.
[44] *Id.*

101. In its announcement, ARG failed to take responsibility for the breach of its POS system. Instead, it put the onus on consumers and the card-issuing financial institutions to identify and resolve any fallout by stating, "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."

102. In March 2017, ARG provided an updated notice finally admitting the Data Breach was a result of malware placed on its POS systems, allowing intruders to access and obtain payment card data (as has occurred in nearly every major retail and fast-food chain data breach.)

103. This payment card data was compromised due to ARG's acts and omissions and its failure to properly protect the Customer Data, despite being aware of recent data breaches impacting other national restaurant chains, including the one at Wendy's.

104. In addition to ARG's failure to prevent the Data Breach, ARG also failed to detect the breach for nearly three months, and only learned of it after being notified by "industry partners" in mid-January.[45]

[45] *Id.*

105. Intruders, therefore, had months to collect payment card data unabated. During this time, ARG failed to recognize its systems had been breached and that intruders were stealing data on millions of payment cards. Timely action by ARG likely would have significantly reduced the consequences of the breach. Instead, ARG took more than three months to realize its systems had been breached, and thus contributed to the scale of the breach and the resulting damages.

106. The Data Breach occurred because ARG failed to implement adequate data security measures to protect its POS networks from the potential danger of a data breach, and failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Customer Data compromised in the Data Breach.

107. While many merchants and vendors have responded to recent breaches by adopting technology and security practices that help make transactions and stored data more secure, ARG has not done so.

108. The Data Breach was caused and enabled by ARG's knowing violation of their obligations to abide by best practices and industry standards in protecting Customer Data.

## H. The Arby's Data Breach Caused Harm and Will Result in Additional Fraud

109. Without detailed disclosure to ARG's customers, consumers, including Consumer Plaintiffs and Class members, have been left exposed, unknowingly and unwittingly, for months to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

110. The ramifications of ARG's failure to keep Consumer Plaintiffs' and Class members' data secure are severe.

111. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[46] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[47]

112. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run

[46] 17 C.F.R § 248.201 (2013).
[47] *Id.*

up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[48]

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

114. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[49]

115. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics

[48] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

[49] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).

("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[50]

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[51]

117. Consumer Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

---

[50] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).
[51] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

## I. Consumer Plaintiffs and Class Members Suffered Damages

118. The Customer Data of Consumer Plaintiffs and Class members is private and sensitive in nature and was left inadequately protected by ARG. ARG did not obtain Plaintiff's and Class members' consent to disclose their Customer Data to any other person as required by applicable law and industry standards.

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

120. ARG had the resources to prevent a breach, having dramatically increased the profitability of Arby's restaurants and its overall annual gross profits in the last few years. ARG made significant expenditures to market its products, modernize its restaurants, and revitalize its brand, but neglected to adequately invest in data security, despite the growing number of POS intrusions and several years of well-publicized data breaches.

121. Had ARG remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, ARG would have prevented intrusion into its POS systems and, ultimately, the theft of its customers' confidential payment card information.

122. As a direct and proximate result of ARG's wrongful actions and inaction and the resulting Data Breach, Consumer Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

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

a. theft of their personal and financial information;

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

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

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

e. the improper disclosure of their Customer Data;

f. loss of privacy;

g. money paid for food purchased at ARG during the period of the Data Breach in that Consumer Plaintiffs and Class members would not have dined at ARG, or at least would not have used their payment cards for purchases, had ARG disclosed that it lacked adequate

systems and procedures to reasonably safeguard customers' financial and personal information and had ARG provided timely and accurate notice of the Data Breach;

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

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

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

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

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

124. ARG has not offered customers any credit monitoring or identity theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Consumer Plaintiffs and Class members are left to their own actions to protect themselves from the financial damage ARG have allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that ARG's actions have created for Plaintiff and Class members, is ascertainable and is a determination appropriate for the trier of fact. ARG have also not offered to cover any of the damages sustained by Plaintiff or Class members.

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

## CHOICE OF LAW

126. Georgia, which seeks to protect the rights and interests of Georgia and other U.S. residents against a company doing business in Georgia, has a greater interest in the claims of Plaintiffs and the Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

127. The principal place of business of ARG, located at 1155 Perimeter Center West, Atlanta, Georgia, is the "nerve center" of its business activities – the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security, and where: a) major policy, b) advertising, c) distribution, d) accounts receivable departments and e) financial and legal decisions originate.

128. ARG's corporate point-of-sale system and IT personnel operate out of and are located at ARG's headquarters in Georgia. PCI-DSS assessments and other duties related to POS systems and data security occur at ARG's Atlanta headquarters.

129. Furthermore, ARG's response to, and corporate decisions surrounding such response to, the Data Breach were made from and in Georgia.

130. ARG's breach of its duty to customers, and Consumer Plaintiffs, emanated from Georgia.

131. Application of Georgia law to a nationwide Class with respect to Consumer Plaintiffs' and the Class members' claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiffs and the nationwide Class.

132. Further, under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia will apply to the common law claims of all Class members.

## CLASS ALLEGATIONS

133. Consumer Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P.

23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seek certification of a Nationwide class defined as follows:

> All persons residing in the United States who made a credit or debit card purchase at any affected Arby's location from October 8, 2016 through January 12, 2017 (the "Nationwide Class").

134. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Consumer Plaintiffs assert claims under the laws of the individual States of Georgia, Tennessee, Connecticut, and Florida, and on behalf of separate statewide classes, defined as follows:

> All persons residing in [Georgia, Tennessee, Connecticut, or Florida] who made a credit or debit card purchase at any affected Arby's location from October 8, 2016 through January 12, 2017 (the "Statewide Classes").

135. Excluded from each of the above Classes are ARG and any of its affiliates, parents or subsidiaries; all employees of ARG; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

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

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

138. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Consumer Plaintiffs at this time, the proposed Class include at least 355,000 customers whose data was compromised in the Arby's Data Breach. 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.

139. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

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

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

c. Whether ARG's security measures to protect their POS systems were reasonable in light of the PCI DSS requirements, FTC data security

recommendations, and other measures recommended by data security experts;

d. Whether ARG was negligent in failing to implement reasonable and adequate security procedures and practices;

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

f. Whether ARG's conduct constituted deceptive trade practices under Georgia law;

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

h. Whether Consumer Plaintiffs and Class members were injured and suffered damages or other acceptable losses because of ARG's failure to reasonably protect its POS systems and data network; and,

i. Whether Consumer Plaintiffs and Class members are entitled to relief.

140. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs Jacqueline Weiss, Joseph Weiss, Ashley Russell, Brett Barnes, and Burnell Rutters are consumers who used their payment cards at affected Arby's locations and had

their cards compromised as a result of the Data Breach. Consumer Plaintiffs' damages and injuries are akin to other Class members and Consumer Plaintiffs seek relief consistent with the relief of the Class.

141. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Consumer Plaintiffs are adequate representatives of the Class because Consumer Plaintiffs are members of the Class and are committed to pursuing this matter against ARG to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Consumer Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Consumer Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

142. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The 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 Consumer Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their

claims against ARG, and thus, individual litigation to redress ARG'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.

143. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). 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.

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

a. Whether ARG failed to timely notify the public of the Breach;

b. Whether ARG owed a legal duty to Consumer Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Customer Data;

c. Whether ARG's security measures to protect is POS systems were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and other measures recommended by data security experts;

d. Whether ARG's failure to adequately comply with PCI DSS standards and/or to institute protective measures beyond PCI DSS standards amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the Customer Data of Plaintiffs and the Class members; and,

f. Whether adherence to PCI DSS requirements, FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

145. Finally, all members of the proposed Classes are readily ascertainable. ARG has access to information regarding which of its restaurants were affected by the Data Breach, the time period of the Data Breach, and which customers were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

**COUNT I**
**BREACH OF IMPLIED CONTRACT**
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)**

146. Consumer Plaintiffs restate and reallege Paragraphs 1 through 132 as if fully set forth herein.

147. ARG solicited and invited Consumer Plaintiffs and Class members to eat at its restaurants and make purchases using their credit or debit cards. Consumer Plaintiffs and Class members accepted ARG's offers and used their credit or debit cards to make purchases at ARG restaurants during the period of the Data Breach.

148. When Consumer Plaintiffs and Class members purchased and paid for ARG's services and food products at ARG using payment cards, they provided their Customer Data, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards. In so doing, Consumer Plaintiffs and Class members entered into mutually agreed-upon implied contracts with ARG pursuant to which ARG agreed to safeguard and protect such information and to timely and accurately notify Consumer Plaintiffs and Class members if their data had been breached and compromised.

149. Consumer Plaintiffs and Class members would not have provided and entrusted their PII and PCD, including all information contained in the magnetic

stripes of their credit and debit cards, to ARG to eat at its restaurants and make purchases in the absence of the implied contract between them and ARG.

150. Consumer Plaintiffs and Class members fully performed their obligations under the implied contracts with ARG.

151. ARG's obligations under the implied contracts were to be executed in Georgia, as its corporate point-of-sale system and IT personnel operate out of and are located at ARG's "nerve center" in Georgia.

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

153. As a direct and proximate result of ARG's breaches of the implied contracts between ARG and Consumer Plaintiffs and Class members, Consumer Plaintiffs and Class members sustained actual losses and damages as described in detail above.

**COUNT II**
**NEGLIGENCE**
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)**

154. Consumer Plaintiffs restate and reallege Paragraphs 1 through 132 as if fully set forth herein.

155. Upon accepting and storing the Customer Data of Consumer Plaintiffs and Class Members in its computer systems and on its networks, ARG undertook and owed a duty to Consumer Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. ARG knew that the Customer Data was private and confidential and should be protected as private and confidential.

156. ARG owed a duty of care not to subject Consumer Plaintiffs, along with their Customer Data, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

157. ARG owed numerous duties to Consumer Plaintiffs and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Customer Data in its possession;

b. to protect Customer Data using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

158. ARG also breached its duty to Consumer Plaintiffs and the Class Members to adequately protect and safeguard Customer Data by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Customer Data. Furthering their dilatory practices, ARG failed to provide adequate supervision and oversight of the Customer Data with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Customer Data of Consumer Plaintiffs and Class Members, misuse the Customer Data and intentionally disclose it to others without consent.

159. ARG knew, or should have known, of the risks inherent in collecting and storing Customer Data, the vulnerabilities of POS systems, and the importance of adequate security. ARG knew about numerous, well-publicized data breaches

within the restaurant industry, including the 2015 breach at Wendy's, restaurants also owned by the parent company of ARG.

160. ARG knew, or should have known, that their data systems and networks did not adequately safeguard Consumer Plaintiffs' and Class Members' Customer Data.

161. ARG breached its duties to Consumer Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Customer Data of Consumer Plaintiffs and Class Members.

162. Because ARG knew that a breach of its systems would damage hundreds of thousands of ARG customers, including Consumer Plaintiffs and Class members, ARG had a duty to adequately protect their data systems and the Customer Data contained thereon.

163. ARG had a special relationship with Consumer Plaintiffs and Class members. Consumer Plaintiffs' and Class members' willingness to entrust ARG with their Customer Data was predicated on the understanding that ARG would take adequate security precautions. Moreover, only ARG had the ability to protect its systems and the Customer Data it stored on them from attack.

164. ARG's own conduct also created a foreseeable risk of harm to Consumer Plaintiffs and Class members and their Customer Data. ARG's misconduct included failing to: (1) secure its point-of-sale systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

165. ARG also had independent duties under state and federal laws that required ARG to reasonably safeguard Consumer Plaintiffs' and Class members' Personal Information and promptly notify they about the data breach.

166. ARG breached its duties to Consumer Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Customer Data of Consumer Plaintiffs and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Consumer Plaintiffs' and Class

members' Customer Data both before and after learning of the Data Breach;

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Consumer Plaintiffs' and Class members' Customer Data had been improperly acquired or accessed.

167. Through ARG's acts and omissions described in this Complaint, including ARG's failure to provide adequate security and its failure to protect Customer Data of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, ARG unlawfully breached its duty to use reasonable care to adequately protect and secure Customer Data of Plaintiff and Class members during the time it was within ARG possession or control.

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

169. ARG breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiff and Class Members and then by failing to provide Plaintiff and Class Members information regarding the breach until February 2017. To date, ARG has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

170. Through ARG's acts and omissions described in this Complaint, including ARG's failure to provide adequate security and its failure to protect Customer Data of Consumer Plaintiffs and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, ARG unlawfully breached its duty to use reasonable care to adequately protect and secure Customer Data of Consumer Plaintiffs and Class members during the time it was within ARG's possession or control.

171. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, ARG prevented Consumer Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

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

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

174. Neither Consumer Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Customer Data as described in this Complaint.

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

**COUNT III**
**NEGLIGENCE PER SE**
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)**

176. Consumer Plaintiffs restate and reallege Paragraphs 1 through 132 as if fully set forth herein.

177. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as ARG, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form part of the basis of ARG's duty in this regard.

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

179. ARG's violation of Section 5 of the FTC Act constitutes negligence *per se*.

180. Consumer Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

181. The harm that occurred as a result of the Arby's Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Consumer Plaintiffs and the Class.

182. As a direct and proximate result of ARG's negligence *per se*, Consumer Plaintiffs and the Class have suffered, and continue to suffer, injuries damages arising from Consumer Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years

to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

**COUNT IV**
**UNJUST ENRICHMENT**
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)**

183. Consumer Plaintiffs restate and reallege Paragraphs 1 through 132 as if fully set forth here.

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

185. ARG knew that Consumer Plaintiffs and Class members conferred a benefit on ARG and accepted and has accepted or retained that benefit. ARG profited from the purchases and used the Customer Data of Consumer Plaintiffs and Class members for business purposes.

186. ARG failed to secure the Customer Data of Consumer Plaintiffs and Class members and, therefore, did not provide full compensation for the benefit the Consumer Plaintiffs and Class members provided.

187. ARG acquired the Customer Data through inequitable means it failed to disclose the inadequate security practices previously alleged.

188. If Consumer Plaintiffs and Class members knew that ARG would not secure their Customer Data using adequate security, they would not have made purchases at Arby's restaurants.

189. Consumer Plaintiffs and Class members have no adequate remedy at law.

190. Under the circumstances, it would be unjust for ARG to be permitted to retain any of the benefits that Consumer Plaintiffs and Class members conferred on it.

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

**COUNT V**
**DECLARATORY JUDGMENT**
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)**

192. Consumer Plaintiffs restate and reallege Paragraphs 1 through 132 as if fully set forth here.

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

194. ARG still possesses Customer Data pertaining to Consumer Plaintiffs and Class members.

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

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

197. Actual harm has arisen in the wake of the Arby's Data Breach regarding ARG's contractual obligations and duties of care to provide data security measures to Consumer Plaintiffs and Class members.

198. Consumer Plaintiffs, therefore, seek a declaration that (a) ARG's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, ARG must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on ARG's systems on a periodic basis, and ordering ARG to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

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

e. purging, deleting, and destroying in a reasonable secure manner Customer Data not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

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

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

**COUNT VI**
**VIOLATION OF GEORGIA FAIR BUSINESS PRACTICES ACT**
**O.C.G.A. § 10-1-390, *ET SEQ*.**
**(ON BEHALF OF CONSUMER PLAINTIFFS AND**
**THE NATIONWIDE CLASS)**

199. Consumer Plaintiffs restate and reallege Paragraphs 1 through 132 as if fully set forth here.

200. Consumer Plaintiffs, as well as Class members are consumers who used their credit or debit cards to purchase food and drink products at Arby's

restaurants owned and operated by ARG. Therefore, Consumer Plaintiffs and Class members have engaged in "consumer transactions" with Defendant ARG pursuant to O.C.G.A. § 10-1-392(10).

201. ARG is engaged in, and their acts and omissions affect, trade and commerce pursuant to O.C.G.A. § 10-1-392(28).

202. As discussed above, ARG's acts, practices, and omissions at issue in this matter were directed and emanated from its headquarters in Georgia.

203. By making purchases from Arby's restaurants owned and operated by ARG, Consumer Plaintiffs and Class members entrusted ARG with their private Customer Data.

204. As alleged herein this Complaint, ARG engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the GFBPA:

a. failure to maintain adequate computer systems and data security practices to safeguard Customer Data;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Customer Data from theft;

c. failure to timely and accurately disclose the Data Breach to Consumer Plaintiffs and Class members;

d. continued acceptance of credit and debit card payments and storage of other personal information after ARG knew or should have known of the security vulnerabilities of the POS systems that were exploited in the Data Breach; and

e. continued acceptance of credit and debit card payments and storage of other personal information after ARG knew or should have known of the Data Breach and before it allegedly remediated the Breach.

205. More specifically, ARG violated the following provisions of the GFBPA:

a. Engaging in in unfair and deceptive acts and practices in the credit and debit card processing services furnished in connection with the sale of goods at Arby's restaurants (O.C.G.A. § 10-1-393(a));

b. Misrepresenting that its services and data systems abided by and had sponsorship, approval, or certification by the Payment Card Industry Security Standards Council (O.C.G.A. § 10-1-393(b)(2));

c. Misrepresenting that its services and data systems had an affiliation, connection, or association with, or certification by, the Payment Card Industry Security Standards Council (O.C.G.A. § 10-1-393(b)(3)); and

d. Misrepresenting that its services and data systems had the sponsorship, approval, characteristics, and benefits by complying with the PCI DSS standards (O.C.G.A. 10-1-393(b)(5)).

206. Furthermore, as alleged above, ARG's failure to secure consumers' Customer Data violates the FTCA and therefore violates the GFBPA.

207. ARG knew or should have known that its computer and POS systems and data security practices were inadequate to safeguard the Customer Data of Consumer Plaintiffs and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

208. ARG knew or should have known that by accepting credit and debit cards as methods of payment its customers would expect that ARG's POS and data systems were secure unless ARG otherwise informed them.

209. Because ARG accepted credit and debit cards as methods of payment its customers, including Plaintiffs and Class members, expected that ARG's POS and data systems were secure and that their Customer Data would be secure.

210. Because ARG accepted credit and debit cards as methods of payment, Consumer Plaintiffs and Class members relied upon ARG to advise customers if its POS and data systems were not secure and, thus, Customer Data could be compromised.

211. Consumer Plaintiffs and Class members were not afforded by ARG equal or ample opportunity to make any inspection to determine ARG's data security or to otherwise ascertain the truthfulness of Defendant's representations and omissions regarding data security, including ARG's failure to alert customers that its POS and data systems were not secure and, thus, were vulnerable to attack.

212. In deciding to use their payment cards for their purchases at ARG-owned and operated restaurants, Consumer Plaintiffs and Class members relied to their detriment upon ARG's representations and omissions regarding data security, including ARG's failure to alert customers that its POS and data systems were not secure and, thus, were vulnerable to attack.

213. Had ARG disclosed to Consumer Plaintiffs and Class members that its POS and data systems were not secure and, thus, vulnerable to attack, Consumer Plaintiffs and Class members would not have used their payment cards at ARG-owned and operated restaurants, and very well may not have made purchases at all at these Arby's locations.

214. As a direct result of their reliance upon ARG to be truthful in its disclosures and non-disclosures regarding the vulnerability of its POS and data systems, Consumer Plaintiffs and Class members used their payment cards to make purchases at ARG-owned and operated restaurants during the Data Breach period

and their Customer Data was compromised causing Plaintiff and Class members to suffer damages.

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

to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

216. Also as a direct result of ARG's knowing violation of the GFBPA, Consumer Plaintiffs and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that ARG engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on ARG's systems on a periodic basis, and ordering ARG to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

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

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

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

217. Consumer Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Consumer Plaintiffs and Class members and the public from ARG's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful

practices. ARG's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

218. Pursuant to O.C.G.A. § 10-1-399(b), at least 30 days prior to bringing this claim, Consumer Plaintiffs have provided ARG with a written demand for relief describing the unfair or deceptive act or practice relied upon and the injury suffered by them. More than 30 days have elapsed since the service of that written demand. No written tender of settlement has been made by ARG.

219. Consumer Plaintiffs and Class members are entitled to a judgment against ARG for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the GFBPA, costs, and such other further relief as the Court deems just and proper.

**COUNT VII**
**(ALTERNATIVELY TO COUNT VI)**
**VIOLATIONS OF THE CONNECTICUT UNFAIR TRADE PRACTICES ACT,**
**C.G.S. §§ 42-110a *et seq.***
**(ON BEHALF OF THE CONNECTICUT STATEWIDE CLASS)**

220. Plaintiffs Jacqueline Weiss and Joseph Weiss ("Connecticut Consumer Plaintiffs"), individually and on behalf of the other Connecticut Statewide Class members, restate and reallege Paragraphs 1 through 132 as if fully set forth here.

221. Connecticut Consumer Plaintiffs and Connecticut Statewide Class Members are consumers who used their credit or debit cards to purchase food and drink products and services at Arby's restaurants owned and operated by ARG. These purchases were made primarily for personal, family, or household purposes.

222. ARG engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of food and drink products to consumers, including Connecticut Consumer Plaintiffs and Connecticut Statewide Class members.

223. ARG engaged in, and its acts and omissions affect, trade and commerce. ARG's acts, practices, and omissions were done in the course of ARG's business of marketing, offering to sell, and selling food and drink products and services throughout the state of Connecticut and the United States.

224. ARG knew or should have known that its computer systems and data security practices were inadequate to safeguard the Customer Data of the Connecticut Statewide Class and that the risk of a data breach was highly likely.

225. ARG knew or should have known that by accepting credit and debit cards as methods of payment its customers would expect that ARG's POS and data systems were secure unless ARG otherwise informed them.

226. ARG operating in Connecticut engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of C.G.S. § 42-110b, including but not limited to the following:

a. failure to maintain adequate computer systems and data security practices to safeguard Customer Data;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Customer Data from theft;

c. failure to timely and accurately disclose the Data Breach to Connecticut Consumer Plaintiffs and Connecticut Statewide Class members;

d. continued acceptance of credit and debit card payments and storage of other personal information after ARG knew or should have known of the security vulnerabilities of the POS systems that were exploited in the Data Breach; and

e. continued acceptance of credit and debit card payments and storage of other personal information after ARG knew or should have known of the Data Breach and before it allegedly remediated the Breach.

227. These unfair acts and practices violated duties imposed by law including but not limited to the FTCA.

228. Had ARG disclosed to Connecticut Consumer Plaintiffs and Connecticut Statewide Class members that its POS and data systems were not secure and, thus, vulnerable to attack Connecticut Consumer Plaintiffs and Connecticut Statewide Class members would not have used their payment cards at ARG-owned and operated restaurants, and very well may not have made purchases at all at these Arby's locations.

229. As a direct and proximate result of ARG's violation of the Connecticut Unfair Trade Practices Act, Connecticut Consumer Plaintiffs and Connecticut Statewide Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Connecticut Consumer Plaintiffs and members of the Connecticut Statewide Class; damages arising from Connecticut Consumer Plaintiffs' and Connecticut Statewide Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit

reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

230. Also as a direct result of ARG's knowing violation of the Connecticut Unfair Trade Practices Act, Connecticut Consumer Plaintiffs and members of the Connecticut Statewide Class are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that ARG engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on ARG's systems on a periodic basis, and ordering ARG to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

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

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

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

231. Connecticut Consumer Plaintiffs bring this action on behalf of themselves and Connecticut Statewide Class members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Connecticut Consumer Plaintiffs and Connecticut Statewide Class members and the public from ARG's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. ARG's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

232. The above unfair and deceptive practices and acts by ARG were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Connecticut Consumer Plaintiffs and Connecticut Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

233. ARG knew or should have known that its computer systems and data security practices were inadequate to safeguard Connecticut Statewide Class members' Personal Information and that risk of a data breach or theft was high.

234. ARG's actions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

235. Connecticut Consumer Plaintiffs and Connecticut Statewide Class members seek relief under C.G.S. §§ 42-110a, *et seq.*, including, but not limited to, damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

**COUNT VIII**
**(ALTERNATIVELY TO COUNT VI)**
**VIOLATIONS OF THE OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq.***
**(ON BEHALF OF THE FLORIDA STATEWIDE CLASS)**

236. Plaintiff Burnell Rutters ("Florida Consumer Plaintiff"), individually and on behalf of the other Florida Statewide Class members, restate and reallege Paragraphs 1 through 132 as if fully set forth here.

237. Florida Consumer Plaintiff and Florida Statewide Class members are consumers who used their credit or debit cards to purchase food and drink products and services at Arby's restaurants owned and operated by ARG. These purchases were made primarily for personal, family, or household purposes.

238. ARG engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of food and drink products to consumers, including Florida Consumer Plaintiff and Florida Statewide Class members.

239. ARG engaged in, and its acts and omissions affect, trade and commerce. ARG's acts, practices, and omissions were done in the course of ARG's business of marketing, offering to sell, and selling food and drink products and services throughout the United States.

240. ARG operating in Florida engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failure to maintain adequate computer systems and data security practices to safeguard Customer Data;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Customer Data from theft;

c. failure to timely and accurately disclose the Data Breach to Florida Consumer Plaintiff and Florida Statewide Class members;

d. continued acceptance of credit and debit card payments and storage of other personal information after ARG knew or should have known of the security vulnerabilities of the POS systems that were exploited in the Data Breach; and

e. continued acceptance of credit and debit card payments and storage of other personal information after ARG knew or should have known of the Data Breach and before it allegedly remediated the Breach.

241. These unfair acts and practices violated duties imposed by laws including by not limited to the FTCA and Fla. Stat. § 501.171(2).

242. As a direct and proximate result of ARG's violation of the Florida Unfair and Deceptive Trade Practices Act, Florida Consumer Plaintiff and Florida Statewide Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Florida Consumer Plaintiffs and Florida Statewide Class members; damages arising from Consumer Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports

and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

243. Also as a direct result of ARG's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Florida Consumer Plaintiff and Florida Statewide Class members are entitled to damages as well as injunctive relief, including, but not limited to:

A. Ordering that ARG engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on ARG's systems on a periodic basis, and ordering ARG to promptly correct any problems or issues detected by such third-party security auditors;

B. Ordering that ARG engage third-party security auditors and internal personnel to run automated security monitoring;

C. Ordering that ARG audit, test, and train its security personnel regarding any new or modified procedures;

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

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

F. Ordering that ARG conduct regular database scanning and securing checks;

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

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

244. Florida Consumer Plaintiff brings this action on behalf of himself and Florida Statewide Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair

information to allow consumers to make informed purchasing decisions and to protect Florida Consumer Plaintiff and Florida Statewide Class members and the public from ARG's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. ARG's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

245. The above unfair and deceptive practices and acts by ARG were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Florida Consumer Plaintiff and Florida Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

246. ARG knew or should have known that its computer systems and data security practices were inadequate to safeguard Florida Statewide Class Members' Personal Information and that risk of a data breach or theft was high.

247. ARG's actions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

248. Florida Consumer Plaintiff and Florida Statewide Class Members seek relief under Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*, including, but not limited to, damages, restitution, injunctive relief, and/or attorneys' fees and costs, and any other just and proper relief.

**COUNT IX**
**(ALTERNATIVELY TO COUNT VI)**
**VIOLATION OF THE TENNESSEE CONSUMER PROTECTION ACT, TENN. CODE ANN. §§ 47-18-101, *et seq*.**
**(ON BEHALF OF THE TENNESSEE STATEWIDE CLASS)**

249. Plaintiff Ashley Russell ("Tennessee Consumer Plaintiff") restates and realleges Paragraphs 1 through 132 as if fully set forth herein.

250. Tennessee Consumer Plaintiff and members of the Tennessee Statewide Class are consumers who used their credit or debit cards to purchase food and drink products and services at Arby's restaurants owned and operated by ARG. These purchases were made primarily for personal, family, or household purposes.

251. ARG engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of food products, goods or services to consumers, including Tennessee Consumer Plaintiff and members of the Tennessee Statewide Class.

252. ARG engaged in, and its acts and omissions affect, trade and commerce. ARG relevant acts, practices and omissions complained of in this action were done in the course of ARG business of marketing, offering for sale and selling food products, goods and services throughout the state of Tennessee and the United States.

253. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-101, *et seq*., prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of Tennessee.

254. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of Tennessee, ARG actions were directed at consumers.

255. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of Tennessee, ARG collected and stored highly personal and private information, including Customer Data belonging to the Tennessee Statewide Class.

256. ARG knew or should have known that its computer systems and data security practices were inadequate to safeguard the Customer Data of the Tennessee Statewide Class and that the risk of a data breach was highly likely.

257. ARG knew or should have known that by accepting credit and debit cards as methods of payment its customers would expect that ARG's POS and data systems were secure unless ARG otherwise informed them.

258. As alleged herein this Complaint, ARG engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, goods or services to consumers in the state of Tennessee, in

violation of Tenn. Code Ann. § 47-18-104, including but not limited to the following:

a. failure to maintain adequate computer systems and data security practices to safeguard Tennessee Statewide Class members' Customer Data;

b. misrepresenting the material fact that ARG would maintain adequate data privacy and security practices and procedures to safeguard Tennessee Statewide Class members' Customer Data from unauthorized disclosure, release, data breaches, and theft in violation of Tenn. Code Ann. § 47-18-104(b)(5) and (9);

c. misrepresenting the material fact that ARG did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the Customer Data of the Tennessee Statewide Class in violation of Tenn. Code Ann. § 47-18-104(b)(5) and (9);

d. failing to disclose, and the misrepresenting the material fact, that ARG computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft in violation of Tenn. Code § 47-18-104(b)(5) and (9);

e. failing to disclose in a timely and accurate manner to the Tennessee Statewide Class the material fact of the nature and extent of the ARG data security breach in violation of Tenn. Code Ann. § 47-18-2107(b); and,

f. continuing to accept credit and debit card payments and storage of other personal information after ARG knew or should have known of the security vulnerabilities of the POS systems that were exploited in the Data Breach; and,

a. continued acceptance of credit and debit card payments and storage of other personal information after ARG knew or should have known of the Data Breach and before it allegedly remediated the Breach.

259. These unfair acts and practices violated duties imposed by law, including but not limited to the FTCA.

260. By engaging in the conduct delineated above, ARG has violated the Tennessee Consumer Protection Act by, among other things:

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

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

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

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

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

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

g. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial. ARG systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of the Tennessee Statewide Class.

261. Furthermore, as alleged above, ARG's failure to secure consumers' Customer Data violates the FTCA and therefore violates the Tennessee Consumer Protection Act.

262. ARG actions in engaging in the conduct delineated above were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Tennessee Statewide Class.

263. Had ARG disclosed to Tennessee Consumer Plaintiff and Tennessee Statewide Class members that its POS and data systems were not secure and, thus, vulnerable to attack, Tennessee Consumer Plaintiff and Tennessee Statewide Class members would not have used their payment cards at ARG-owned and operated restaurants, and very well may not have made purchases at all at these Arby's locations.

264. As a direct result of ARG violation of the Tennessee Consumer Protection Act, Tennessee Consumer Plaintiff and Tennessee Statewide Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Tennessee Consumer Plaintiff and Tennessee Statewide Class members; damages arising from Tennessee Consumer Plaintiff's and Tennessee Statewide Class members' inability to use their payment card because the compromised cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late

fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

265. As a result of ARG violations of the Tennessee Consumer Protection Act, the Tennessee Statewide Class is entitled to, and seek, injunctive relief, including but not limited to:

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

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

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

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

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

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

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

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

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

266. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of ARG alleged herein, the Tennessee Statewide Class seeks relief under Tenn. Code Ann. § 47-18-109, including, but not limited to, actual damages, treble damages for each willful or knowing violation, injunctive relief, and attorneys' fees and costs.

## REQUEST FOR RELIEF

**WHEREFORE**, Consumer Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against ARG as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Consumer Plaintiffs and their Counsel to represent the Nationwide Class, or in the alternative the separate Statewide Classes;

b. For equitable relief enjoining ARG from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Consumer Plaintiffs' and Class members' Customer

Data, and from refusing to issue prompt, complete and accurate disclosures to the Consumer Plaintiffs and Class members;

c. For equitable relief compelling ARG to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of Customer Data compromised;

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

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

Such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMAND**

Plaintiff demands a jury trial on all issues so triable.

This 19th day of March 2018.

**BARNES LAW GROUP, LLC**

/s John R. Bevis
Roy E. Barnes
Ga. Bar No. 039000
John R. Bevis
Ga. Bar No. 056100

**FARUQI & FARUQI, LLP**

Robert W. Killorin
Ga. Bar No. 17775
Stuart J. Guber
Ga. Bar No. 141879
Timothy J. Peter *

J. Cameron Tribble
Ga. Bar No. 754759

31 Atlanta Street
Marietta, GA 30060
Tel: (770) 227-6375
Fax: (770) 227-6373
roy@barneslawgroup.com
bevis@barneslawgroup.com
ctribble@barneslawgroup.com

101 Greenwood Avenue, Suite 600
Jenkintown, Pennsylvania 19046
Phone: (215) 277-5770
Fax: (215) 277-5771
sguber@faruqilaw.com
tpeter@faruqilaw.com

*Co-Lead Counsel*
*for Consumer Plaintiffs and the Proposed Class*

**MORGAN & MORGAN**
**COMPLEX LITIGATION GROUP**
John Yanchunis *
Marisa Glassman *

201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
Fax: (813) 223-5402
jyanchunis@forthepeople.com
mglassman@forthepeople.com

**EVANGELISTA WORLEY, LLC**
James M. Evangelista
Ga. Bar No. 707807
David J. Worley
Ga. Bar No. 776665

8100A Roswell Road Suite 100
Atlanta, GA 30350
Tel: (404)205-8400
Fax: (404)205-8395
jim@ewlawllc.com
david@ewlawllc.com

*Co-Liaison Counsel*
*for Consumer Plaintiffs and the Proposed Class*

** Pro Hac Vice*

CERTIFICATE OF SERVICE

I hereby certify that on March 19, 2018, I caused **PLAINTIFFS' FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**, to be served via the Court's CM/ECF system, which will automatically send notice of such filing to all attorneys of record.

This the 19th day of March, 2018.

Respectfully submitted,

*s/ John A. Yanchunis*
John A. Yanchunis
**MORGAN & MORGAN**
**COMPLEX LITIGATION GROUP**
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
Fax: (813) 223-5402
jyanchunis@forthepeople.com