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

ASHLEY RUSSELL, individually and on behalf of all others similarly situated, Plaintiff, v. ARBY'S RESTAURANT GROUP, INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff Ashley Russell ("Plaintiff"), individually and on behalf of the Classes defined below of similarly situated persons, alleges the following against Arby's Restaurant Group, Inc. ("ARG" or "Defendant") based upon personal knowledge with respect to herself 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. Plaintiff brings this class action case against ARG for its failure to secure and safeguard its customers' credit and debit card numbers and other payment card data ("PCD"), and other personally identifiable information ("PII") which ARG

collected at the time Plaintiff made a restaurant purchase at ARG (collectively, "Customer Data"), and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class members that their Customer Data had been stolen and precisely what types of information were stolen.

2. In February of 2017, ARG acknowledged that customers at its corporate restaurant locations 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 malware to access the point-of-sale ("POS") systems at approximately 1,000 ARG corporate restaurant locations to gain access to customers' debit and credit card information, including credit card numbers.

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

5. 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.

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

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

7. The Data Breach was the inevitable result of ARG's inadequate approach to data security. The deficiencies in ARG's data security were so significant that the malware installed by the hackers remained undetected and intact for months.

8. ARG disregarded the rights of Plaintiff 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 take available steps to prevent and stop the breach from ever happening, and failing to disclosure to its customers the material facts that it did not have adequate computer systems and security practices to safeguard Customer Data.

9. As a result of the ARG data breach, the Customer Data of the Class members has been exposed to criminals for misuse.

10. Plaintiff retains a significant interest in ensuring that her Customer Data, which remains in the possession of ARG, is protected from further breaches, and seek to remedy the harms she has suffered on behalf of herself and similarly situated consumers whose Customer Data was stolen as a result of the ARG data

breach. Plaintiff asserts claims against ARG for violations of the Tennessee Consumer Protection Act ("TUTPA"), breach of implied contract, and negligence.

11. Plaintiff, on behalf of herself and similarly situated consumers, seeks 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

12. 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. Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

13. This Court has personal jurisdiction over Defendant because ARG maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant intentionally avails itself of this jurisdiction by marketing and selling products and services from Georgia to millions of consumers nationwide.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District.

PARTIES

15. Plaintiff Ashley Russell is a resident of the state of Tennessee. On or around December 3, 2016, Plaintiff Ashley Russell visited an ARG restaurant located at 601 Old Hickory Road in Jackson, Tennessee and purchased food items using her debit card issued by her bank. Shortly thereafter, Ms. Russell was contacted by her bank 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 placing a freeze on her account and it would send her a new debit card. Ms. Russell was not able to withdraw money before the bank froze her account. Ms. Russell had to travel out-of-state and because she could not access her account or use her debit card, 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, account freeze and replacement card.

16. Plaintiff would not have used her debit card to make purchases at ARG—indeed, she would not have shopped at ARG at all during the period of the ARG data breach—had ARG told her that it lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft.

17. Plaintiff suffered actual injury from having her Customer Data compromised and stolen in and as a result of the ARG data breach.

18. Plaintiff suffered actual injury and damages in paying money to and purchasing products from ARG during the ARG data breach that she would not have paid had ARG disclosed that it lacked computer systems and data security practices adequate to safeguard customers' Customer Data.

19. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his or her Customer Data – a form of intangible property that Plaintiff entrusted to ARG for the purpose of purchasing its products and that was compromised in and as a result of the ARG data breach.

20. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her Customer Data being placed in the hands of criminals who have already misused such information stolen in the ARG data breach via sale of Plaintiff' and Class members' Customer Data on the Internet black market, as evidenced by the compromise of Ms. Russell's debit card. Plaintiff has a continuing interest in ensuring that her private information, which remains in the possession of ARG, is protected and safeguarded from future breaches.

21. Plaintiff is likely to purchase food or services from ARG with a debit card in the future if ARG's data security was improved to protect against future data breaches.

22. 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.

23. ARG's restaurant system consists of over 3,300 corporate- owned and franchisee locations across the U.S. and worldwide. Approximately one third of these are corporate-owned restaurants. ARG restaurants accept payment for their goods and services through a POS system, through which customers swipe credit and debit cards to pay.

STATEMENT OF FACTS

I. ARG and Its Customer Data Collection Practices

24. ARG was founded in 1964 and is America's first nationally franchised sandwich restaurant. ARG's restaurant system consists of over 3,300 restaurants worldwide. In 2016, ARG produced system-wide sales of more than $3.6 billion. A large majority of these sales at ARG locations are made to customers using credit or debit cards.

25. When ARG 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 completion of the payment.

26. At all relevant times, ARG was well-aware, or reasonably should have been aware, that the Customer Data it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

II. Stolen Customer Data is Valuable to Hackers and Thieves

27. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches by retailers, ARG maintained an insufficient and inadequate system to protect the PII of Plaintiff and class members.

28. Legitimate organizations and the criminal underground alike recognize the value in PII. 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 from 38 million users."[1]

29. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as retailers, ARG's approach to maintaining the privacy of Plaintiffs' and Class members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

III. ARG Failed to Comply with Industry Standards

30. Payment Card Data ("PCD") is heavily regulated. 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.[2]

31. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed

---

[1] 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).

[2] *Payment Card Industry Data Security Standard* v3.2, p. 5 (April 2016) available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1492014699947 (last accessed April 10, 2017).

to protect account data."[3] PCI DSS sets the minimum level of what must be done, not the maximum.

32. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, impose the following mandates on ARG[4]:

PCI Data Security Standard – High Level Overview

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

33. 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.

[3] *Id.*
[4] *Id.*

34. 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.[5]

35. 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.

IV. ARG Failed to Upgrade its Payment Systems to Use EMV Technology

36. The payment card industry also sets rules requiring all businesses to upgrade to new card readers that accept EMV chips. 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

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

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

37. 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.

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

39. 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.

V. ARG Failed to Comply With FTC Requirements

40. In 2016, the Federal Trade Commission ("FTC") updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[6] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer

[6]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).

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.

41. The FTC has supplemented those guidelines with is publication Start With Security.[7] In these guidelines, 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 verify that third-party service providers have implemented reasonable security measures.

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

---

[7] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 10, 2017).

43. ARG's failure to follow the guidelines recommended by the FTC and failure to have reasonable data security measures in place constitute an unfair act or practice within the meaning of Section 5 of the FTC Act, 15 U.S.C. § 45.

VI. The ARG Data Breach

44. As early as 2009, the predecessor entity of Defendant 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)

45. 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. In fact, Wendy's, one of ARG's parent companies, had a malware-driven breach of its POS systems that began in the fall of 2015, affected more than 1,000 Wendy's locations, and continued for at least nine months. Based on the data breaches within the restaurant industry, the significant breach and Wendy's and Defendant's own acknowledgment of the risks, ARG knew or should have known that it was at high risk for a similar malware data breach.

46. In or around October 20, 2016, hackers installed malicious malware to access POS systems at approximately 1,000 ARG corporate-owned restaurant locations nationwide, allowing the thieves to download and steal copies of ARG customers' Customer Data.

47. ARG estimates that the breach occurred between October 20, 2016 and January 12, 2017.[8]

48. PSCU, an organization that handles 800 credit unions, was the first to report the breach, reporting that both Track 1 and Track 2 data may have been

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

compromised in the ARG data breach. Track 1 and Track 2 data normally includes credit and debit card information such as the cardholder name, primary account number, expiration date, and, in certain instances, PIN number. The PSCU alert also indicated that at least 355,000 credit and debit cards were compromised.[9]

49. This private customer information was compromised due to ARG's acts and omissions and its failure to properly protect the Customer Data, despite being aware of the recent data breaches impacting other national restaurant chains and one of its parent companies.

50. 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.[10]

51. The Data Breach occurred because ARG failed to implement adequate data security measures to protect its POS network from the potential danger of a data breach, and failed to implement and maintain adequate systems to detect and prevent the breach and resulting harm that it has caused.

---

[9] https://krebsonsecurity.com/2017/02/fast-food-chain-arbys acknowledges- breach/ (last visited on April 10, 2017)

[10] *Id.*

52. Had ARG implemented and maintained adequate safeguards to protect Customer Data, deter the hackers, and detect the data breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented.

53. In permitting the Data Breach to occur, ARG breached its implied agreement with customers to protect their personal and financial information and violated industry standards.

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

55. While many retailers 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.

56. ARG 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.

VII. The ARG Data Breach Caused Harm and Will Result in Additional Fraud

57. Without detailed disclosure to ARG's customers, consumers, including Plaintiff 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.

58. The ramifications of ARG's failure to keep Plaintiff's and Class members' data secure are severe.

59. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] 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."[12]

60. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. The information ARG's compromised, including Plaintiff' identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the FTC. Identity theft occurs when someone uses another's PII, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

---

[11] 17 C.F.R § 248.201 (2013).
[12] *Id.*

61. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[13]

62. Identity thieves can use personal information, such as that of Plaintiff 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. Some of this activity may not come to light for years.

63. 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 ("BJS")

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

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.[14]

64. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[15]

65. 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.[16]

66. Plaintiff 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

---

[14] Victims of Identity Theft, 2014 (Sept. 2015) *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (April 10, 2017).
[15] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).
[16] GAO, Report to Congressional Requesters, at p.29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

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.

VIII. Plaintiff and Class Members Suffered Damages

67. The Data Breach was a direct and proximate result of ARG's failure to properly safeguard and protect Plaintiff' 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 Plaintiff' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

68. Plaintiff's and Class members' PII 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 PII to any other person as required by applicable law and industry standards.

69. As a direct and proximate result of ARG's wrongful actions and inaction and the resulting Data Breach, Plaintiff 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.

70. ARG's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff' 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 Plaintiff's 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 Plaintiff 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; 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,

k. 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.

71. 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, Plaintiff and Class members are left to their own actions to protect themselves

from the financial damage ARG has 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 has also not offered to cover any of the damages sustained by Plaintiff or Class members.

72. While the Customer Data of Plaintiff and members of the Class has been stolen, ARG continues to hold Customer Data of consumers, including Plaintiff and Class members. Particularly because ARG has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff 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.

CLASS ALLEGATIONS

73. Plaintiff 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 ARG affected location from October 20, 2016 through January 12, 2017 (the "Nationwide Class").

74. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide class, Plaintiff assert claims for and on behalf of a separate statewide class for Tennessee as follows:

> All persons residing in Tennessee who made a credit or debit card purchase at any ARG affected location from October 20, 2016 through January 12, 2017 (the "Tennessee Subclass").

75. The Nationwide Class and Tennessee Subclass are individually referred to as "Class" and collectively referred to as the "Classes."

76. Excluded from each of the Classes is Defendant and any of its parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

77. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

78. Plaintiff is a member of both Classes.

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

80. **Numerosity. Fed. R. Civ. P. 23(a)(1).** The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Classes include at least 355,000 customers whose data was compromised in the ARG data breach.

81. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

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

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

c. Whether ARG knew or should have known that its computer systems were vulnerable to attack;

d. Whether ARG has an implied contractual obligation to use reasonable security measures;

e. Whether ARG has complied with any implied contractual obligation to use reasonable security measures;

f. Whether ARG conduct constituted deceptive trade practices under Tennessee law;

g. Whether ARG's conduct, including its 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 Plaintiff and Class members;

h. Whether ARG's breaches of its legal duties caused Plaintiff and the Class members to suffer damages;

i. Whether Plaintiff and Class members are entitled to recover damages; and

j. whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

82. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of those of other Class members because ARG failed to safeguard Plaintiff's information, like that of every other Class member.

83. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

84. **Superiority. Fed. R. Civ. P. 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy

because joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

85. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, ARG's violations of law inflicting substantial damages in the aggregate would go un-remedied.

86. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). ARG has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

87. 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 Class members' Customer Data was accessed, compromised, or stolen in the Data Breach;

b. Whether (and when) Defendant knew about the Data Breach before it was announced to the public and failed to timely notify the public of the Breach;

c. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Customer Data;

d. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Customer Data;

e. Whether Defendant's conduct was an unlawful or unfair business practice under Tenn. Code Ann. §§ 47-18-101.;

f. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

g. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and Class members' Customer Data secure and prevent the loss or misuse of that information;

h. Whether Defendant failed to take commercially reasonable steps to safeguard the Customer Data of Plaintiffs and the Class members and thereby knowingly divulged the Customer Data of Plaintiffs and the Class members while carried and maintained on Defendant's data systems

i. Whether an implied contract existed between Defendant and Plaintiffs and the Class members and the terms of that implied contract; and,

j. Whether Defendant breached the implied contract;

88. 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 breach, which customers were potentially affected, as well as the addresses and other contact information for members of the Classes, which can be used for providing notice to the Class members.

COUNT I
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class)

89. Plaintiff restates and realleges Paragraphs 1 through 88 as if fully set forth herein.

90. ARG solicited and invited Plaintiff and Class members to eat at its restaurants and make purchases using their credit or debit cards. Plaintiff 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.

91. When Plaintiff and Class members made and paid for purchases of ARG's services and products in connection with their meals at ARG properties, 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, Plaintiff and Class members entered into implied contracts with ARG pursuant to which ARG agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members if their data had been breached and compromised.

92. Each purchase at ARG restaurants made by Plaintiff and Class members using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with ARG under which ARG agreed to safeguard and protect the Customer Data of Plaintiff and Class members, including all information contained in the magnetic stripe of Plaintiff' and Class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

93. Plaintiff 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.

94. Plaintiff and Class members fully performed their obligations under the implied contracts with ARG.

95. ARG breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the PII and PCD of Plaintiff 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.

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

COUNT II
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

97. Plaintiff restates and realleges Paragraphs 1 through 88 as if fully set forth herein.

98. Upon accepting and storing the Customer Data of Plaintiff and Class Members in its computer systems, ARG undertook and owed a duty to Plaintiff 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.

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

100. 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.

101. ARG also breached its duty to Plaintiff and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Customer Data. Furthering its dilatory practices, ARG failed to provide adequate supervision and oversight of the Customer Data with which it was and is 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 Plaintiff and Class Members, misuse the Customer Data and intentionally disclose it to others without consent.

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

103. 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 Plaintiff 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.

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

105. Upon information and belief, ARG improperly and inadequately safeguarded Customer Data of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access ARG failure to take proper security measures to protect sensitive Customer Data of Plaintiff 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 Plaintiff and Class members.

106. ARG failed to take proper security measures to protect Customer Data of Plaintiff and Class members.

107. 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 Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive Customer Data had been compromised.

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

109. As a direct and proximate cause of ARG's conduct, Plaintiff 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 Plaintiff and Class Members; damages arising from Plaintiff's 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
Violation of The Tennessee Consumer Protection Act,
Tenn. Code. Ann. §§ 47-18-101, et seq.
(On behalf of the Tennessee Consumer Protection Class)

110. Plaintiff restates and realleges Paragraphs 1 through 88 as if fully set forth here.

111. Plaintiff Ashley Russell and members of the Tennessee Consumer Protection Class (collectively the "Tennessee Consumer Protection Class") are consumers who used their credit or debit cards to purchase food and drink products for personal, family and household purposes from ARG locations in Tennessee.

112. 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 the Tennessee Consumer Protection Class.

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

114. 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.

115. 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's actions were directed at consumers.

116. 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 Consumer Protection Class.

117. ARG knew or should have known that its computer systems and data security practices were inadequate to safeguard the Customer Data of the Tennessee Consumer Protection Class and that the risk of a data breach was highly likely and/or that the risk of the data breach being more extensive than originally disclosed was highly likely.

118. ARG should have disclosed this information regarding its computer systems and data security practices because ARG was in a superior position to know the true facts related to the defect, and the Tennessee Consumer Protection Class could not reasonably be expected to learn or discover the true facts.

119. 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. failing to adequately secure the Customer Data of the Tennessee Consumer Protection Class;

b. failing to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information;

c. misrepresenting the material fact that ARG would maintain adequate data privacy and security practices and procedures to safeguard Customer

Data from unauthorized disclosure, release, data breaches, and theft in violation of Tenn. Code Ann. § 47-18-104(b)(5) and (9);

d. 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 Consumer Protection Class in violation of Tenn. Code Ann. § 47-18-104(b)(5) and (9);

e. failing to disclose, and misrepresenting the material fact, that ARG's 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);

f. failing to disclose in a timely and accurate manner to the Tennessee Consumer Protection 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,

g. continuing to accept 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 remedied the breach.

120. 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 Consumer Protection Class.

121. ARG's actions in engaging in the conduct delineated above were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Tennessee Consumer Protection Class.

122. As a direct result of ARG's violation of the Tennessee Consumer Protection Act, the Tennessee Consumer Protection Class has suffered actual damages that include:

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

b. theft of their personal and financial information by criminals;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with unauthorized use of their financial accounts;

e. 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;

f. costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, canceling and activating

payment cards, and shopping for credit monitoring and identity theft protection;

g. the certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and being already misused;

h. impairment to their credit scores and ability to borrow and/or obtain credit; and,

i. the continued risk to their personal information, which remains on ARG's insufficiently secured computer systems.

123. As a result of ARG's violations of the Tennessee Consumer Protection Act, the Tennessee Consumer Protection 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's 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's 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.

124. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of ARG alleged herein, the Tennessee Consumer Protection 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, Plaintiff, 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 Nationwide Class, or alternatively the Statewide Consumer Protection Class, as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class, or alternatively the Statewide Consumer Protection Class;

b. For equitable relief enjoining ARG from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Customer Data, and from refusing to

issue prompt, complete and accurate disclosures to the Plaintiff and Class members;

c. For equitable relief compelling ARG to use appropriate methods and policies with respect to consumer data collection, storage and safety and to disclose with specificity to Class members the type of PII and PCD compromised;

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

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

Dated: April 28, 2017

s/ Roy E. Barnes
Roy E. Barnes
Georgia Bar No. 039000
John R. Bevis
Georgia Bar No. 056110
J. Cameron Tribble
Georgia Bar No. 754759

THE BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, Georgia 30060
Telephone: (770) 227-6375
Facsimile: (770) 227-6373
roy@barneslawgroup.com
bevis@barneslawgroup.com
ctribble@barneslawgroup.com

John Yanchunis*
Florida Bar Number 324681
Marisa Glassman*
Florida Bar Number 111991
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@forthepeople.com
mglassman@forthepeople.com

Jean Sutton Martin*
North Carolina Bar Number 25703
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road, Suite 225
Wilmington, North Carolina
Telephone: (910) 292-6676
jean@jsmlawoffice.com

Paul C. Whalen (PW-1300)*
LAW OFFICE OF PAUL C. WHALEN, P.C.
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
paul@paulwhalen.com

Jasper D. Ward IV*
JONES WARD PLC
312 S. Fourth Street
Louisville, KY 40202
Telephone: (502) 882-6000
jasper@jonesward.com

Brian P. Murray*
GLANCY PRONGAY & MURRAY LLP
122 East 42nd Street, Suite 2920
New York, NY 10168
Telephone: (212) 682-5340
bmurray@glancylaw.com

* *pro hac vice* application forthcoming

Attorneys for Plaintiffs and the Proposed Class

JS44 (Rev. 11/16 NDGA)

CIVIL COVER SHEET

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

I. (a) PLAINTIFF(S)

ASHLEY RUSSELL, individually and on behalf of all others similarly situated,

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

DEFENDANT(S)

ARBY'S RESTAURANT GROUP, INC.

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____
(IN U.S. PLAINTIFF CASES ONLY)

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

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

Roy E. Barnes, John R. Bevis and J. Cameron Tribble
BARNES LAW GROUP, LLC
31 Atlanta Street, Marietta, GA 30060
770-227-6375; roy@barneslawgroup.com;
bevis@barneslawgroup.com; ctribble@barneslawgroup.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

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

III. CITIZENSHIP OF PRINCIPAL PARTIES

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

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

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

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

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

Class Action pursuant to 28 U.S.C. § 1332(d)(2) whereby Defendant, among other things, failed to adequately protect Plaintiff's credit data in violation of statutory and common law.

(IF COMPLEX, CHECK REASON BELOW)

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

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23 DEMAND $_____

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

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE Thomas Thrash DOCKET NO. 1:17-cv-01035-TWT

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

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

s/ Roy E. Barnes 4/28/2017

SIGNATURE OF ATTORNEY OF RECORD DATE