

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

JACQUELINE WEISS and JOSEPH WEISS, individually and on behalf of all others similarly situated,)	Case No.:
)	
Plaintiffs,)	CLASS ACTION COMPLAINT
)	
v.)	<u>DEMAND FOR JURY TRIAL</u>
)	
ARBY’S RESTAURANT GROUP, INC.)	
)	
Defendant.)	
)	
)	
)	
)	
)	
)	
)	

CLASS ACTION COMPLAINT

Plaintiffs Jacqueline Weiss and Joseph Weiss (collectively the “Plaintiffs”), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Arby’s Restaurant Group, Inc. (“ARG” or “Defendant”) 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. This is a consumer class action against ARG for its failure to secure and safeguard its customers' credit and debit card numbers and other payment card data, and other personally identifiable information which ARG collected at the time Plaintiffs and other Class members¹ made purchases at ARG (collectively, "Customer Data").

2. 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 locations² to gain access to customers' debit and credit card information, including credit card numbers.

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

4. 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, 2017.³

5. ARG disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and

¹ Classes defined *infra* in Paragraphs 57-59.

² According to ARG, only corporate-owned restaurants were impacted. <http://arbys.com/security/> (last visited on March 22, 2017).

³ <https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/> (last visited on March 22, 2017).

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 disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard Customer Data.

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

7. As a result of the ARG data breach, the Customer Data of the Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members as a direct result of the ARG data breach include:

- a. unauthorized charges on their debit and credit card accounts;
- 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 ARG 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 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 ARG 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 Plaintiffs' and Class members' information on the Internet black market;
- h. 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 with the mutual understanding that ARG would safeguard Plaintiffs' and Class members' data against theft and not allow access to and misuse of their information by others;
- i. money paid for products and services purchased at ARG stores during the period of the ARG data breach, in that Plaintiffs and Class members would not have shopped at ARG had ARG disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Customer Data; and
- j. continued risk to their Customer Data which remains in the possession of ARG and which is subject to further breaches so long as ARG fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data in its possession.

8. The injuries to the Plaintiffs and members of the Classes were directly and proximately caused by ARG's failure to implement or maintain adequate data security measures for Customer Data. ARG failed to take steps to employ adequate

security measures despite recent, well-publicized data breaches at large national retail and restaurant chains, including P.F. Chang's, Wendy's, Dairy Queen, and Noodles & Company. Furthermore, ARG exacerbated the situation by failing to detect the data breach earlier. Had ARG detected the breach earlier, less data would have been stolen and customers would have been able to take earlier action to mitigate their damages.

9. Plaintiffs retain a significant interest in ensuring that their Customer Data, which 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 ARG data breach. Plaintiffs assert claims against ARG for violations of the Connecticut's Unfair Trade Practices Act ("CUTPA"), breach of implied contract, and negligence.

10. 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

11. 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. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

12. 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.

13. 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

14. Plaintiffs Jacqueline Weiss and Joseph Weiss are residents of Glastonbury, Connecticut and were Connecticut residents during the period of the ARG data breach. On November 20, 2016, Plaintiffs purchased food at an ARG corporate store located at 3206 Berlin Turnpike, Newington, CT 06111, with a joint Fidelity Visa credit card which was swiped through an ARG point-of-sale payment device. ARG has confirmed that this location has been affected by the

breach.⁴ In or around December 2016, Plaintiffs discovered thousands of dollars in unauthorized charges on the Fidelity Visa credit card used at the affected ARG location, and were forced to cancel that credit card as a result. Plaintiffs expended time contacting the credit card company and attempting to resolve the issues caused by the theft of their identity. During the period of time Plaintiffs were awaiting their replacement credit card, Plaintiffs were required to use alternative sources of funds to make purchases, thereby foregoing credit card reward points and/or cash-back rewards and experiencing actual damages.

15. Plaintiffs would not have used their credit or debit cards to make purchases at ARG—indeed, they would not have shopped at ARG at all during the period of the ARG data breach—had ARG told them that it lacked adequate computer systems and data security practices to safeguard customers’ Customer Data from theft.

16. Each of the Plaintiffs suffered actual injury from having his or her Customer Data compromised and stolen in and as a result of the ARG data breach.

17. Each of the Plaintiffs suffered actual injury and damages in paying money to and purchasing products from ARG during the ARG data breach that they would not have paid had ARG disclosed that it lacked computer systems and data security practices adequate to safeguard customers’ Customer Data.

⁴ <http://arbys.com/security/> (last visited on March 22, 2017).

18. Each of the Plaintiffs 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 each of the Plaintiffs entrusted to ARG for the purpose of purchasing its products and that was compromised in and as a result of the ARG data breach.

19. Each of the Plaintiffs has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his or 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 Plaintiffs' and Class members' Customer Data on the Internet black market. 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.

20. Plaintiffs are likely to purchase food or services from ARG with a credit or debit card in the future if ARG's data security was improved to protect against future data breaches.

21. 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'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. Background

22. The 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.⁵ A large majority of these sales at ARG locations are made to customers using credit or debit cards.

23. 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.

24. 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.

5

<http://www.businesswire.com/news/home/20170125005654/en/Arby%E2%80%99s-Achieves-Record-Annual-Revenue-FY16-Same-Store> (last visited on March 22, 2017)

25. Stolen Customer Data is a valuable commodity. A “cyber black-market” exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. The 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.

26. 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.”⁶

27. Furthermore, 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.

28. At all relevant times, ARG was well-aware, or reasonably should have been aware, of the importance of safeguarding its customers’ Customer Data and

⁶ <https://www.consumer.ftc.gov/articles/0271-warning-signsidentity-theft> (last visited March 22, 2017).

of the foreseeable consequences that would occur if its data security systems were breached, specifically, including the significant costs that would be imposed on customers as a result of a breach.

29. At all relevant times, ARG was well-aware, or reasonably should have been aware, that hackers had been targeting the payment card data of major U.S. retailers, including national restaurant chains, for many years. Indeed, in the years leading up to the ARG breach, retailer such as Home Depot and Target and restaurant chains including P.F. Chang's, Wendy's, Dairy Queen, and Noodles & Company were subject to well-publicized data breaches. In a number of these breaches, hackers were able to install data-stealing malware on the restaurants' POS systems.

30. Due to the extensive network of financial institutions involved in credit and debit transactions and the large volume of daily transactions, financial institutions and credit card processing companies have issued rules and standards governing the basic protective measures that merchants must take to ensure that a customer's valuable Customer Data is safeguarded.

31. Furthermore, the requirements of industry standards, the FTC Act, and other authorities imposed a duty on ARG to use adequate care to protect its customers' sensitive Customer Data:

32. *Industry Standards:*

- a. The payment card industry (MasterCard, Visa, Discover Financial Services, and American Express), long before the ARG data breach, issued Card Operating Regulations that: (1) are binding on ARG; (2) required ARG to protect cardholder data and prevent its unauthorized disclosure; (3) prohibited ARG from storing such data, even in encrypted form, longer than necessary to process the transaction; and (4) mandated that ARG comply with industry standards.
- b. The payment card industry has also set rules requiring all businesses, including ARG, to upgrade to new card readers that accept EMV chips. EMV chip technology uses embedded computer chips instead of magnetic stripes to store payment card data. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the hackers making it much more difficult for criminals to profit from what is stolen.

- c. The set deadline for businesses to transition their systems from magnetic-stripe to EMV technology was October 1, 2015, a deadline ARG, on information and belief, did not meet. According to Creditcards.com, “Following an Oct. 1, 2015 deadline created by major U.S. credit card issuers MasterCard, Visa, Discover and American Express, the liability for card-present fraud shifted to whichever party is the least EMV-compliant in a fraudulent transaction.”⁷
- d. Under the Card Operating Regulations that are binding on Defendant, businesses accepting payment cards but not meeting the October 1, 2015 deadline agree to be liable for damages resulting from any data breaches.
- e. Further, the Payment Card Industry Security Standards Council promulgates minimum standards which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standards (“PCI DSS”). PCI DSS is the industry standard governing the

⁷ <http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php> (last visited on March 22, 2017).

security of payment card data, although it sets the minimum level of what must be done, not the maximum.

- f. PCI DSS 3.1, the version of the standards in effect at the time of the ARG data breach, sets detailed and comprehensive requirements for satisfying each of the following 12 “high-level” mandates:⁸

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

- g. Among other things, PCI DSS required ARG to properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data on a need-to-know basis; establish a process to identify and timely

⁸ https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf (last visited on March 22, 2017).

fix security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and encrypt payment card data at the point of sale.

- h. 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.⁹
- i. At all relevant times, ARG was fully aware of its obligations to protect Customer Data in light of its participation in the payment card processing networks and its daily collection and transmission of tens of thousands of sets of payment card data. ARG was also fully aware that customers such as Plaintiffs were entitled to, and did, rely on ARG to use adequate care and follow PCI DSS requirements in protecting their sensitive Customer Data from data thieves.
- j. While compliance with the PCI DSS is required as a minimum guarantee of protection, PCI DSS compliance in and of itself is insufficient. For example, Georgia Weidman, CTO and founder of Shevirah (a company that tests data security for retailers and other

⁹ PCI Security Standards Council LLC, PCI DSS Requirements and the Security Assessment Procedures, Version 3.1, 38 (Apr. 2015).

merchants), has stated that “[e]very company that has been spectacularly hacked in the last three years has been PCI complaint Obviously, based on that evidence, while a good step in the right direction, PCI is not sufficient to protect against breaches.”¹⁰

33. *FTC Act:*

- a. Pursuant to the Federal Trade Commission (“FTC”), the failure to employ reasonable and adequate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. §45.
- b. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses, noting 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 for installing vendor approved patches to correct security problems. The guidelines also recommend that businesses consider using an

¹⁰ <http://www.eweek.com/security/eddie-bauer-reveals-it-was-the-victim-of-a-pos-breach> (last visited on March 22, 2017).

intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

- c. The FTC also has published a document entitled “FTC Facts for Business,” which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.¹¹
- d. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

34. *State Statutes:*

- a. The state of Connecticut has enacted the Connecticut Unfair Trade Practices Act (“CUTPA”), which prohibits unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. Conn. Gen. Stat. § 42-110(b), *et seq.*

¹¹ <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business> (last visited on March 22, 2017).

II. The ARG Data Breach

35. 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.

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

36. Further, in the years following this acknowledgment of the risks, massive data breaches plagued the restaurant industry, including national restaurant chains such as Wendy's, Noodles & Co., and P.F. Chang's. Each of these restaurant chains had employed the Aloha POS system at the time of breach, the same system employed by ARG during the ARG breach. Based on those data breaches and Defendant's own acknowledgment of the risks, ARG knew or should

have known that the Aloha POS system it employed was at high risk for a similar malware data breach.

37. 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.

38. ARG estimates that the breach occurred between October 20, 2016 and January 12, 2017.¹²

39. 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 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.¹³

40. 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.

¹² <http://arbys.com/security/> (last visited on March 22, 2017).

¹³ <https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/> (last visited on March 22, 2017)

41. 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.¹⁴

42. The 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.

43. Had ARG implemented and maintained adequate safeguards to protect the 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.

44. 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.

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

45. The ARG data breach was a direct and proximate result of ARG failure to properly safeguard and protect Plaintiffs' and Class members' Customer Data from unauthorized access, use, and disclosure, as required by state and federal

¹⁴ *Id.*

regulations, industry practices, and statutory law, including ARG failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

46. As a result of the breach, the Customer Data of Plaintiffs and Class members has been exposed to criminals for misuse.

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

48. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁵ 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."¹⁶

49. Thieves are already using the Customer Data stolen from ARG to commit actual fraud, as evidenced by the unauthorized charges to Plaintiffs' credit card, as alleged herein.

¹⁵ 17 C.F.R § 248.201 (2013).

¹⁶ *Id.*

50. The injuries suffered by Plaintiffs and the proposed Classes (and which they will continue to suffer) as a direct result of the ARG data breach include, but are not limited, to those listed in Paragraph 7.

51. In addition to fraudulent charges and damage to their credit, many victims spent or will spend substantial time and expense relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Addressing their inability to withdraw funds linked to compromised accounts;
- e. Removing withdrawal and purchase limits on compromised accounts;
- f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- g. Resetting automatic billing instructions; and
- h. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

52. Examples of the foregoing harms caused to ARG customers as a direct and foreseeable consequence of ARG's conduct include the experiences of Plaintiffs, who experienced unauthorized charges on their credit card.

53. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Customer Data is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:¹⁷

[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.

54. There is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning ARG customers could be at risk of fraud and identity theft for years into the future.

55. Therefore, as a result of ARG's conduct, Plaintiff and Class members now have to deal with the repercussions of fraud, identity theft, and constant surveillance of their personal and financial records for years to come.

56. Despite acknowledging the repercussions from its wrongful actions and inaction and the resulting the breach, ARG has not offered customers any recourse such as free credit monitoring. As a result, Plaintiffs and Class members are left to their own actions to protect themselves from the financial damage ARG

¹⁷ Government Accounting Office. *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, 29 (June 2007), <http://www.gao.gov/new.items/d07737.pdf> (last visited March 22, 2017).

has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that ARG actions have created for Plaintiffs 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 Plaintiffs or Class members.

CLASS ALLEGATIONS

57. 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), and (b)(3), Plaintiffs seek to certify a class of 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”).

58. Plaintiffs also seek to certify a class of all persons residing in the Connecticut who made a credit or debit card purchase at any ARG affected location from October 20, 2016 through January 12, 2017 (the “Connecticut Subclass”).

59. The Nationwide Class and Connecticut Subclass are individually referred to as “Class” and collectively referred to as the “Classes.”

60. 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.

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

62. Plaintiffs are members of both Classes.

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

64. **Numerosity.** The proposed Classes include at least 355,000 customers whose data was compromised in the ARG data breach. While the precise number of Class members has not yet been determined, the massive size of the ARG data breach indicates that joinder of each member would be impracticable.

65. **Commonality.** 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 conduct constituted deceptive trade practices under Connecticut law.

- d. Whether ARG 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 Plaintiffs and Class members;
- e. whether ARG's breaches of its legal duties caused Plaintiffs and the Class members to suffer damages;
- f. whether Plaintiffs and Class members are entitled to recover damages; and
- g. whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

66. **Typicality.** Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs and Class members were injured through ARG's uniform misconduct and their legal claims arise from the same core practices employed or omitted by ARG.

67. **Adequacy.** Plaintiffs are adequate representatives of the proposed Classes because their interests do not conflict with the interests of the Class members they seek to represent. Plaintiffs' counsel are experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have successfully prosecuted similarly massive retail data breach cases.

68. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against ARG. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

69. 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.

70. Finally, all members of the proposed Classes are readily ascertainable. ARG has access to information regarding which of its restaurants were affected by the 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
Violation of Connecticut Unfair Trade Practices Act (“CUTPA”),
Conn. Gen. Stat. § 42-110a, *et seq.*

(On Behalf of Plaintiffs and Connecticut Subclass)

71. Plaintiffs restate and reallege Paragraphs 1 through 70 as if fully set forth herein.

72. Plaintiffs and Connecticut Subclass members are consumers who used their credit or debit cards to purchase food and drink products from ARG.

73. ARG engages in in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiffs and Connecticut Subclass members.

74. ARG is engaged in, and its acts and omissions affect, trade and commerce. ARG acts, practices, and omissions were done in the course of ARG's business of marketing, offering for sale, and selling goods and services throughout Connecticut.

75. ARG's conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices (collectively, "Deceptive Trade Practices"), including, among other things, ARG's:

- 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. 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 that were exploited in the breach; and
- d. 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 fixed the breach.

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

77. By engaging in such Deceptive Trade Practices, ARG has violated the CUTPA.

78. As a direct result of ARG violation of CUTPA, Plaintiffs and Connecticut Subclass members damages, including, but not limited, to those listed in Paragraphs 50-51.

79. Also as a direct result of ARG violation of CUTPA, Plaintiffs and Connecticut Subclass members are entitled to 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.

80. Because of ARG's Deceptive Trade Practices, Plaintiffs and the Connecticut Subclass members are entitled to relief, including restitution of the costs associated with the data breach, disgorgement of all profits accruing to ARG because of its Deceptive Trade Practices, attorneys' fees and costs, declaratory relief, and a permanent injunction enjoining ARG from its Deceptive Trade Practices.

81. Plaintiffs bring this action on behalf of themselves and Connecticut Subclass members for the relief requested and for the public benefit in order to promote the public interests in the provision of truthful, nondeceptive information to allow consumers to make informed purchasing decisions and to protect Plaintiffs and Connecticut Subclass members and the public from ARG unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful

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

82. Plaintiffs will provide notice of this action and a copy of this Complaint to the appropriate Attorneys General pursuant to Conn. Gen. Stat. § 42-110g(c).

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and all Classes)

83. Plaintiffs restate and reallege Paragraphs 1 through 70 as if fully set forth herein.

84. ARG solicited and invited Plaintiffs and Class members to eat at its restaurants and make purchases using their credit or debit cards. Plaintiffs and Class members accepted ARG offers and used their credit or debit cards to make purchases at ARG restaurants from October 20, 2016 through January 12, 2017.

85. When Plaintiffs and Class members made and paid for purchases of ARG services and products from October 20, 2016 through January 12, 2017, they provided their Customer Data to ARG. In so doing, Plaintiffs and Class members entered into implied contracts with ARG pursuant to which ARG agreed to safeguard and protect such information and to timely detect any breaches of their Customer Data.

86. Plaintiffs and Class members would not have provided and entrusted their Customer Data with ARG in the absence of the implied contract between them and ARG.

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

88. ARG breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect the Customer Data of Plaintiffs and Class members and by failing to timely detect the data breach within a reasonable time.

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

COUNT III
Negligence
(On Behalf of Plaintiffs and all Classes)

90. Plaintiffs restate and reallege Paragraphs 1 through 70 as if fully set forth herein.

91. By accepting and storing the Customer Data of Plaintiffs and Class Members in its computer systems, ARG undertook and owed numerous duties to Plaintiffs and to members of the Classes, including the duty 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. ARG also knew about numerous, well-publicized data breaches by other national retailers.

92. Furthermore, the law imposes an affirmative duty on ARG to timely detect unauthorized access and theft of the Customer Data.

93. ARG breached the duties it owed to Plaintiffs and Class members in numerous ways, including:

- a. by creating a foreseeable risk of harm through the misconduct previously described;
- b. by failing to implement adequate security systems, protocols and practices sufficient to protect the Customer Data both before and after learning of the data breach;
- c. by failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the data breach; and
- d. by failing to timely detect the data breach;

94. 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 Plaintiffs and Class members during the time it was within ARG's possession or control.

95. Neither Plaintiffs nor the other Class members contributed to the data breach and subsequent misuse of their Customer Data as described in this Complaint.

96. But for ARG's wrongful and negligent breach of the duties it owed Plaintiffs and Class members, their Customer Data either would not have been compromised or they would have been able to prevent some or all of their damages.

97. As a direct and proximate cause of ARG's negligent conduct, Plaintiffs and the Class suffered damages including, but not limited to those stated in Paragraphs 50-51. Moreover, 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. Accordingly, Plaintiffs and the Class members have suffered injury and will continue to do so, and are entitled to damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes, respectfully request that the Court enter judgment in their favor that:

- A. certifies the Classes requested, appoints the Plaintiffs as class representatives of the applicable Classes and appoint the Counsel representing Plaintiffs as Class counsel;
- B. awards the Plaintiffs and Class members appropriate monetary relief, including actual damages, restitution, and disgorgement,
- C. on behalf of Plaintiffs and the Classes, enter an injunction against ARG's Deceptive Trade Practices and requiring it to implement and maintain adequate security measures, including the measures specified above to ensure the protection of Plaintiffs' and Class members' information, which remains in the possession of ARG;
- D. orders ARG to pay the costs involved in notifying the Class members about the judgment and administering the claims process;
- E. awards Plaintiffs and the Classes pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
- F. awards such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all issues so triable.

Dated: March 22, 2017

Respectfully Submitted,

/s/ James M. Evangelista

James M. Evangelista

Ga. Bar No. 707807

David J. Worley

Ga. Bar No. 776665

EVANGELISTA WORLEY, LLC

8100A Roswell Road

Suite 100

Atlanta, GA 30350

Phone: (404)205-8400

Fax: (404)205-8395

jim@ewlawllc.com

david@ewlawllc.com

Robert W. Killorin

Ga. Bar No. 417775

Attorney at Law

5587 Benton Woods Drive

Atlanta, GA 30342

(404) 847-0617

rwk@bellsouth.net

Stuart J. Guber

Ga. Bar No. 141879

Timothy J. Peter

(pro hac vice forthcoming)

FARUQI & FARUQI, LLP

101 Greenwood Avenue, Suite 600

Jenkintown, Pennsylvania 19046

Phone: (215) 277-5770

Fax: (215) 277-5771

sguber@faruqilaw.com

tpeter@faruqilaw.com

Counsel for Plaintiffs

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)

JACQUELINE WEISS and JOSEPH WEISS, individually and on behalf of all others similarly situated,

DEFENDANT(S)

ARBY'S RESTAURANT GROUP, INC.

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

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)

Evangelista Worley LLC
8100A Roswell Road, Suite 100
Atlanta, GA 30350
(404)205-8400
jim@ewlawllc.com; david@ewlawllc.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION (PLACE AN "X" IN ONE BOX ONLY)

- 1 U.S. GOVERNMENT PLAINTIFF
2 U.S. GOVERNMENT DEFENDANT
3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
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 Plaintiffs' 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

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

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))

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

IMMIGRATION - "0" MONTHS DISCOVERY TRACK

- 462 NATURALIZATION APPLICATION
- 465 OTHER IMMIGRATION ACTIONS

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK

- 870 TAXES (U.S. Plaintiff or Defendant)
- 871 IRS - THIRD PARTY 26 USC 7609

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

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

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

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

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

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK

- 410 ANTITRUST
- 850 SECURITIES / COMMODITIES / EXCHANGE

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 370 OTHER FRAUD
- 371 TRUTH IN LENDING
- 380 OTHER PERSONAL PROPERTY DAMAGE
- 385 PROPERTY DAMAGE PRODUCT LIABILITY

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

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK

- 896 ARBITRATION (Confirm / Vacate / Order / Modify)

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK

- 422 APPEAL 28 USC 158
- 423 WITHDRAWAL 28 USC 157

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK

- 820 COPYRIGHTS
- 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK

- 830 PATENT

*** 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)

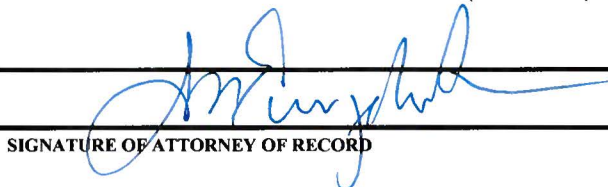
VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE Amy Totenberg DOCKET NO. 1:17-cv-00514-AT

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.



3/22/2017

SIGNATURE OF ATTORNEY OF RECORD

DATE

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Arby's Faces Another Data Breach Lawsuit](#)
