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

MIDWEST AMERICA FEDERAL CREDIT UNION, on behalf of itself and all others similarly situated, Plaintiff, vs. ARBY'S RESTAURANT GROUP, INC., Defendant.	Case No.

CLASS ACTION COMPLAINT

Plaintiff Midwest America Federal Credit Union brings this action on behalf of itself and all others similarly situated against Defendant Arby's Restaurant Group, Inc. ("Arby's" or "Defendant"), and states:

NATURE OF THE CASE

1. Despite the growing threat of computer system intrusion, Defendant systematically failed to comply with industry standards and its statutory and common law duties to protect the payment card data of its customers.

2. Defendant's systemic failure exposed its customers' payment cards from October 25, 2016 to January 19, 2017, and allowed hackers to steal that data and misuse it for various purposes.

3. Had Defendant put reasonable processes and procedures in place, it would have had a reasonable chance to prevent the breach. In fact, Defendant's data practices were so deficient that its customers' data was exposed for almost three months and Defendant failed to detect any issues.

4. The costs and financial harm caused by Defendant's negligent conduct is borne primarily by financial institutions, like Plaintiff, that issued the payment cards compromised in this data breach. These costs include, but are not limited to, cancelling and reissuing compromised cards and reimbursing their members for fraudulent charges. Industry sources estimate that the fraudulent charges associated with this breach at Arby's have been more concentrated than in other recent data breaches (*e.g.*, Target, Home Depot and Wendy's), causing Plaintiff and other members of the Class to suffer much greater losses.

5. This class action is brought on behalf of financial institutions throughout the country to recover the costs that they and others similarly situated have been forced to bear as a direct result of the Defendant's data breach and to

obtain other equitable relief. Plaintiff asserts claims for negligence, and declaratory and injunctive relief.

JURISDICTION AND VENUE

6. This Court has original jurisdiction of this Action pursuant to the Class Action Fairness Act, 28 U.S.C §1332 (d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and at least some members of the proposed Class have a different citizenship from Defendant. There are more than 100 putative class members.

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

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

PARTIES

9. Plaintiff Midwest America Federal Credit Union is a federally chartered credit union with its principal place of business located in Fort Wayne, Indiana.

10. Plaintiff is a VISA payment card issuer and received a CAMS alert around the beginning of the week of February 5, 2017. As a result of the Defendant's actions and the breach of its data systems, Plaintiff has suffered, and continues to suffer, injury, including, inter alia, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

11. Defendant Arby's Restaurant Group, Inc. is a Delaware corporation with its principal place of business located in Atlanta, Georgia.

12. Defendant is a restaurant business that accepts payment for its goods and services through a point-of-sale ("POS") network. Consumers swipe payment cards, which are issued by Plaintiff and the Class, at Defendant's POS terminals to effectuate payment for Defendant's goods and services.

STATEMENT OF FACTS

13. Recently, financial institutions have experienced an unprecedented number of Compromised Account Management System ("CAMS") alerts on their members' accounts from VISA and Account Data Compromise Alerts ("ADC alerts") on their members' accounts from MasterCard. CAMS and ADC alerts typically are issued by VISA and MasterCard when there is some event that jeopardizes the security of a financial institution's customers' accounts.

14. Numerous financial institutions have traced the large number of alerts issued for their customers' accounts and discovered a common thread—Defendant.

15. The number of CAMS and ADC alerts received by many financial institutions have been among the largest (meaning most cards compromised) CAMS or ADC alerts they have ever received for a single event.

16. The alert Plaintiff received estimates the "exposure window" for the breach of Defendant's computer systems runs from October 25, 2016 to January 19, 2017, meaning Defendant failed to prevent or stop hackers from accessing its system and stealing cardholder data for almost three months.

17. The alert further indicates that both Track 1 and Track 2 data may have been compromised in the data breach. Track 1 and Track 2 data normally includes

credit and debit card information such as cardholder name, primary account number, expiration date, and in certain instances PIN number.

18. Defendant still has not made an offical public announcement regarding the breach of its data processing systems approximately four months since the breach began and one month after it ended.

19. The breach of Defendant's data systems occurred through Defendant's POS network, where hackers installed malware that allowed them to steal payment card data from remote locations as a card was swiped for payment.

20. The breach was made possible because Defendant disregarded the security of its POS network and the potential danger of a data breach, and failed to put in place reasonable systems and procedures to prevent the harm that its actions have caused.

21. Defendant knew the danger of not safeguarding its POS network as various high profile data breaches have occurred in the same way, including data breaches of Target, Home Depot, and, most recently, Wendy's.

22. Despite this knowledge, Defendant acted unreasonably and failed to adequately and reasonably protect the data of its customers.

23. Defendant's failure is particularly egregious because various state and federal statutes obligate Defendant to act reasonably in protecting the data of the members of Plaintiff and the Class.

24. First, the payment card industry (MasterCard, VISA, Discover, and American Express), long before the beach of Defendant's data systems, issued Card Operating Regulations that: (1) are binding on Defendant; (2) required Defendant to protect cardholder data and prevent its unauthorized disclosure; (3) prohibited Defendant from storing such data, even in encrypted form, longer than necessary to process the transaction; and (4) mandated Defendant comply with industry standards.

25. Second, the payment card industry set rules requiring all businesses, including Defendant, to upgrade to new card readers that accept EMV chips. EMV chip technology uses imbedded 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.

26. The set deadline for businesses to transition their systems from magnetic-stripe to EMV technology was October 1, 2015, a deadline Defendant, on information and belief, did not meet.

27. 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.

28. Third, 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 Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.

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

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

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

31. Fourth, according the Federal Trade Commission ("FTC"), 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

32. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an 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.

33. 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.

34. 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.

35. Fifth, several states have enacted data breach statutes that require merchants to use reasonable care to guard against unauthorized access to consumer

information, such as California Civil Code § 1798.81.5(b) and Wash. Rev. Code § 19.255, or that otherwise impose data security obligations on merchants, such as Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64. States have also adopted unfair and deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. Moreover, most states have enacted statutes requiring merchants to provide notice if their data security systems are breached. These statutes, implicitly or explicitly, support the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

36. Defendant's failure to employ practices and procedures reasonably capable of securing the cardholder data of the members of Plaintiff and the Class violated all of these statutory- and industry-imposed obligations and caused substantial damage to Plaintiff and the Class.

37. Indeed, the fact that cardholder data was left exposed for close to three months and the fact that Defendant continuously failed to detect this vulnerability demonstrates its complete lack of procedural and other safeguards with respect to its customers' data.

38. Plaintiff and the Class were required to act immediately to mitigate the massive fraudulent transactions being made on payment cards that they had issued,

while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but Plaintiff and class members are not. Financial institutions bear primary responsibility for reimbursing members for fraudulent charges on the payment cards they issue.

39. As a result of the Defendant's data breach, Plaintiff and class members have been forced to cancel and reissue payment cards, change or close accounts, notify members that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to class members and Plaintiff—as well as the account numbers on the face of the cards—were devalued.

40. The financial damages suffered by Plaintiff and members of the class are massive and continue to increase.

41. As a result of the data breach, Plaintiff is incurring significant costs associated with, among other things, notifying members of issues related to the Data Breach, closing out and opening new customer/member accounts, reissuing members' cards, and/or refunding members' losses resulting from the unauthorized use of their accounts.

CLASS ALLEGATIONS

42. Plaintiff brings this action on behalf of herself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seeks certification of the following Class:

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

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

44. **Numerosity**: All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

45. **Commonality and Predominance**: All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3)'s predominance requirement are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. Whether Defendant engaged in the misconduct alleged;

b. Whether Defendant owed a duty to Plaintiff and the class members and whether Defendant violated that duty;

c. Whether Plaintiff and the class members were injured and suffered damages or other ascertainable loss as a result of Defendant's conduct; and

d. Whether Plaintiff and the class members are entitled to relief and the measure of such relief.

46. **Typicality**: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having issued payment cards that were compromised in the data breach of Defendant's data systems. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendant's conduct.

47. **Adequacy**: All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because it is a member of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to represent. Plaintiff is committed to pursuing this matter for the Class with

the Class' collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type, and Plaintiff intends to prosecute this action vigorously. Plaintiff and its counsel will fairly and adequately protect the Class's interests.

48. **Superiority**: The superiority requirement of Fed. R. Civ. P. 23(b)(3) is satisfied. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

49. **Injunctive and Declaratory Relief**: All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

COUNT I
Negligence

50. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

51. Defendant owed a duty to Plaintiff and the members of the class to take reasonable care in cardholder data, and to timely notify Plaintiffs in the case of a data breach. This duty arises from multiple sources.

52. At common law, Defendant owed a duty to Plaintiff and the Class because it was foreseeable that Defendant's data systems and the cardholder data those data systems processed would be targeted by hackers. It also was foreseeable that such hackers would extract cardholder data from Defendant's systems and misuse that information to the detriment of Plaintiff and the class members, and that Plaintiff and the Class would be forced to mitigate such fraud or such potential fraud by cancelling and reissuing payment cards to their members and reimbursing their members for fraud losses.

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

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

55. Defendant also is obligated to perform its business operations in accordance with industry standards, including the PCI DSS, to which Defendant is bound. The industry standards create yet another source of obligations that mandate Defendant to exercise reasonable care with respect to Plaintiff and the Class.

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

57. Upon information and belief, the specific negligent acts and omissions committed by Defendant include, but are not limited to, some or all of the following:

a. failure to delete cardholder information after the time period necessary to authorize the transaction;

b. failure to employ systems to protect against malware;

c. failure to regularly update its antivirus software;

d. failure to maintain an adequate firewall;

e. failure to track and monitor access to its network and cardholder data;

f. failure to limit access to those with a valid purpose;

g. failure to encrypt cardholder data at the point-of-sale;

h. failure to transition to the use of EMV technology;

i. failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

j. failure to assign a unique ID to each individual with access to its systems;

k. failure to automate the assessment of technical controls and security configuration standards;

l. failure to adequately staff and fund its data security operation;

m. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

n. failure to recognize red flags signaling that Defendant's systems were inadequate, and that as a result, the potential for a massive data breach was increasingly likely;

o. failure to recognize that hackers were stealing Customer Data from its network while the data breach was taking place; and

p. failure to disclose the data breach in a timely manner.

58. In connection with the conduct described above, Defendant acted wantonly, recklessly, and with complete disregard for the consequences.

59. As a direct and proximate result of Defendant's conduct, Plaintiff and the class members have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of

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

60. Because no statutes of other states are implicated, Georgia common law applies to Plaintiff and the Class's negligence claim.

COUNT II
Negligence *Per Se*

61. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

62. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, restaurants and other businesses such as Defendant of failing to use reasonable measures to protect cardholder data. The FTC publications and orders described above also form the basis of Defendant's duty.

63. Defendant violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect cardholder data and not complying with applicable industry standards, including PCI DSS as described in detail

previously in this complaint. Defendant's conduct was particularly unreasonable given the nature and amount of cardholder data it obtained and stored and the foreseeable consequences of a data breach at a national restaurant, including specifically the immense damages that would result to consumers and financial institutions.

64. Defendant's violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence per se.

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

66. Moreover, the harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the class members.

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

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

68. Because no statutes of other states are implicated, Georgia common law applies to Plaintiff and the Class's negligence per se claim.

COUNT III
Declaratory and Injunctive Relief

69. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

70. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

71. An actual controversy has arisen in the wake of the data breach at issue regarding Defendant's common law and other duties to act reasonably with respect

to safeguarding the cardholder data of the members of Plaintiff and the Class. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and Defendant denies such allegations. Additionally, Plaintiff continues to suffer injury as additional fraud and other illegal charges are being made on payment cards Plaintiff and the class members have issued.

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

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

b. Defendant breached this legal duty by failing to employ reasonable measure to secure its customers' personal and financial information;

c. Defendant's breach of its legal duty proximately caused the data breach; and

d. Banks, credit unions, and other institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Defendant's data breach are legally entitled to recover the costs they incurred from Defendant.

73. The Court also should issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its customers' personal and financial information. Specifically, this injunction should, among other things, direct Defendant to:

a. utilize industry standard encryption to encrypt transmission of cardholder data at the point-of-sale and at all other times;

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

d. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test its systems for security vulnerabilities, consistent with industry standards;

g. comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and

h. install all upgrades recommended by manufacturers of security software and firewalls used by Defendant.

74. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Defendant's data systems. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant's data systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

75. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendant suffers another massive data breach, Plaintiff and the members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable data security measures is relatively minimal and Defendant has a pre-existing legal obligation to employ such measures.

76. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

77. Wherefore, Plaintiff, on behalf of itself and on behalf of the other members of the Class, requests that this Court award relief against Defendant as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and its counsel as Class Counsel;

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

c. Enter a declaratory judgment in favor of Plaintiff and the Class as described above;

d. Grant Plaintiff and the Class the injunctive relief requested above;

e. Awarding attorneys' fees and costs; and

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

JURY TRIAL DEMANDED

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

Dated: February 10, 2017

s/ Gary F. Lynch

Gary F. Lynch
Jamisen Etzel
Kevin Abramowicz
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com
kabramowicz@carlsonlynch.com

Thomas A. Withers
GILLEN WITHERS & LAKE, LLC
8 E. Liberty Street
Savannah, GA 31401
Telephone: 912.447.8400
Facsimile: 912.629-6347
twithers@gwllawfirm.com

Anthony C. Lake
GILLEN WITHERS & LAKE, LLC
3490 Piedmont Road, N.E.
One Securities Centre, Suite 1050
Atlanta, GA 30305
Telephone: 404.842.9700
Facsimile: 404.842.9750
aclake@gwllawfirm.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Suite 2200
100 Washington Avenue South
Minneapolis, MN 55401-2159
Telephone 612-339-6900
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Attorneys for Plaintiff