NIQA

$400

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

2019 DEC 20 P 5:43

JENNIFER COHEN, on Behalf of Herself and All Others Similarly Situated

v.

WAWA, INC.

) CLASS ACTION COMPLAINT

)USDC-EDPA
CIV CLERK

FILED
DEC 20 2019
KATE BARKMAN, Clerk
By Dep. Clerk

19 6064

CLASS ACTION COMPLAINT

Plaintiff, through undersigned counsel, files on behalf of herself and all persons similarly situated, this Class Action Complaint, alleging the following based on personal knowledge, investigation of counsel and review of public documents. Among other things, as to allegations regarding the Plaintiff and on information and belief as to other allegations.

INTRODUCTION

1. This is a civil action seeking monetary damages, restitution and declaratory relief from Defendant WAWA, Inc. ("WAWA") arising from a data breach announced to the public on December 19, 2019 ("the Data Breach").

2. Plaintiff alleges that WAWA failed to secure and safeguard personal information ("Personal Information") and payment card or other financial information ("Financial Information") (collectively, "Private Information"[1]), that WAWA collected and maintained, and

[1] As defined herein and used throughout this Complaint, "Private Information" includes all information exposed by the data breach, including but not limited to portions of a victim's name, address, postal code, shopping preferences, phone numbers, email addresses, dates of birth, Social Security number, tax identification number, bank account number, credit card number, debit card number, credit scores, credit limits, account balances, payment history, and transaction data.

that WAWA failed to provide timely and adequate notice to Plaintiff and other Class members with details regarding what Private Information had been stolen.

3. At different points in time starting around March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. By April 22, 2019, this malware was present on most store systems.

4. On December 10, 2019, WAWA's IT Department identified this malware. By December 12, 2019, it is alleged that it was blocked and contained.

5. Upon information and belief, an unknown third party ("hacker") took advantage of glaring weaknesses and vulnerabilities in the company's data security systems. WAWA's security protocols were so deficient the breach continued for up to nine months while WAWA failed to even detect it.

6. While the hacker was the perpetrator of the breach, its occurrence was inevitable. WAWA's systemic incompetence and a lackluster approach to data security has existed within the company for years and is ingrained in its culture from the top down. WAWA's failure to seriously address data security persisted despite warnings in the marketplace and the known existence of other numerous, high-profile data breaches at other major American corporations, including Capital One, Home Depot, Target, Michaels and Equifax, all of which should have alerted WAWA of the need to revamp and enhance its inadequate data security practices.

7. Plaintiff's Private Information was exposed by WAWA. She seeks to recover damages and equitable relief on behalf of herself and all others similarly situated in the United States.

JURISDICTION AND VENUE

8. This Court has federal question subject-matter jurisdiction pursuant to 28 U.S.C. § 1331, because Plaintiff alleges that WAWA violated the FCRA.

9. In addition, this Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (1) the Class consists of more than 100 members and (2) the amount at issue is more than $5 million exclusive of interest and costs.

10. This Court has jurisdiction over WAWA because it is a Pennsylvania company with its principal headquarters here, it regularly conducts business in Pennsylvania, has sufficient minimum contacts in Pennsylvania and has intentionally availed itself of this jurisdiction by marketing and selling products in Pennsylvania and other consumers nationwide.

11. Venue in this Court is appropriate pursuant to 28 U.S.C. § 1391(a) because a substantial part of the events, acts, or omissions giving rise to the claims occurred in this District.

PARTIES

12. The Plaintiff brings this action on behalf of herself and those similarly situated across the United States and within their States or Territories of residence, including specifically in New Jersey, Pennsylvania, Delaware, Maryland, Virginia, Florida, and Washington, D.C.

13. As with the rest of the millions of victims of the data breach, WAWA through its actions described herein leaked, disbursed, or furnished Private Information to unknown cyber criminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

14. Plaintiff Jennifer Cohen is a U.S. resident and citizen of the Commonwealth of Pennsylvania, living in Philadelphia. Upon information and belief, her Private Information was compromised in the Data Breach. Before the announcement of the breach, Plaintiff was a regular customer of WAWA for coffee and other products, goes to a number of WAWA stores in the greater Philadelphia area and had made purchases there on numerous occasions from March to

December of 2019. Like millions of other WAWA customers, she used a payment card to make purchases at WAWA.

15. WAWA failed to safeguard the privacy and security of the plaintiff's information. Plaintiff would not have submitted her Private Information had they known of WAWA's inadequate data security practices. Given the highly sensitive nature of the information stolen, Plaintiff remains at a substantial and imminent risk of future harm.

16. Plaintiff is just one of many individuals that have been impacted by the Data Breach.

17. Defendant Wawa, Inc. is a Pennsylvania corporation with its principal place of business at Red Roof, 260 W. Baltimore Pike in Wawa, Pennsylvania 19063. WAWA is a food market operating the website https://www.wawa.com/. WAWA employs almost 37,000 people in New Jersey, Pennsylvania, Delaware, Maryland, Virginia, Florida, and Washington, D.C. WAWA has a registered agent for service of process: CT Corporation System, 116 Pine Street, Suite 320, Harrisburg, Pennsylvania.

CLASS ACTION ALLEGATIONS

18. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Fed. R. Civ. P. 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance and superiority requirements of Rule 23.

19. The proposed class is defined as:

> All natural persons in the United States, within the applicable statute of limitations preceding the filing of this action to the date of class certification, whose Private Information was compromised as a result of the Data Breach.

20. The Class asserts claims against WAWA for violation of the FCRA (Count 1), negligence (Count 2) and negligent misrepresentation (Count 3). The Nationwide Class also requests a declaratory judgment (Count 4).

21. Excluded from the Nationwide Class is WAWA and any of its parents, affiliates, or subsidiaries as well as any successors in interest or assigns of WAWA and the Judge assigned this litigation.

22. Upon information and belief, Plaintiff is a member of the Class, as defined above.

23. The members of the above Class are readily ascertainable and WAWA has access to addresses and other contact information that may be used for providing adequate and thorough notice to class members.

24. The members of the class are so numerous that joinder of all members would be impracticable. Plaintiff is informed and believe---based in part upon WAWA's press releases — that there are hundreds of thousands of class members. Those individuals' names and addresses are available from WAWA's records, and class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

25. There are substantial questions of law and fact common to the classes that predominate over questions affecting only individual Class members including, but not limited to, the following:

a. Whether WAWA owed a duty to the Plaintiff and the class to adequately protect Private Information;

b. Whether WAWA breached its duty to protect Private Information by failing to provide adequate security;

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

d Whether WAWA failed to take adequate and reasonable measures to ensure its data systems were protected;

e. Whether WAWA failed to take available steps to prevent and stop the Data Breach from happening;

f. Whether WAWA's conduct (or lack thereof) was the direct and proximate cause of the Data Breach of its systems, which resulted in the loss or disclosure of Private Information;

g. Whether WAWA improperly retained transaction data beyond the period of time permitted by law;

h. Whether Defendant unreasonably delayed in notifying affected customers of the Data Breach and whether the belated notice was adequate;

i. Whether WAWA negligently failed to inform the Plaintiff and the Class regarding the vulnerabilities of its data protection systems, measures and practices;

j. Whether WAWA's conduct amounted to violations of the FCRA (15 USC §§ 1681, *et seq.*), and/or state data breach or privacy statutes;

k. Whether the Plaintiff and the Class suffered injury as a result of WAWA's conduct (or lack thereof);

l. Whether the Plaintiff and the Class are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief; and

m. What is the appropriate measure of damages sustained by the Plaintiff and the Class?

26. Plaintiff's claims are typical of the Class. The same events and conduct that give rise to Plaintiff's claims are identical to those that give rise to the claims of every other class member because Plaintiff has suffered harm as a direct and proximate cause of the same, specific Data Breach described herein.

27. Plaintiff will fairly and adequately represent the interests of the class. Plaintiff has retained counsel who are experienced and qualified in prosecuting complex class action and data breach litigation similar to this one and Plaintiff intends to prosecute this action vigorously. The class members' interests will be fairly and adequately protected by Plaintiff and her counsel. Neither Plaintiff nor her attorneys have any interest contrary to or conflicting with those of other members of the Class.

28. The prosecution of separate actions by individual class members seeking declaratory and injunctive relief pursuant to Rule 23(b)(2) would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for WAWA. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other class members and impair their interests. WAWA has acted and/or refused to act on grounds generally applicable to the class, making final injunctive relief or corresponding declaratory relief appropriate.

29. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the other class members' claims is economically unfeasible and procedurally impracticable. Litigating the claims of the class together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and unnecessary expense to the parties and the courts.

30. Even if class members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

COMMON FACTUAL ALLEGATIONS

A. What WAWA Does

31. WAWA is primarily a brick and mortar convenience store, food market and a seller of gasoline. WAWA accepts payment for its services via payment cards at all of its stores.

B. WAWA Discovers the Breach and Takes Action

32. On or around December 19, 2019, TechCruch and other media outlets reported that WAWA suffered a data breach that compromised its payment systems. *See, i e.* https://www.newsweek.com/wawa-data-breach-2019-how-check-if-you-have-been-affected-1478437 (last visited December 20, 2019).

33. Wawa CEO Chris Gheysens issued an Open Letter to Customers on December 19, 2019. *See* https://www.wawa.com/alerts/data-security (last visited December 20, 2019). The letter says that:

> Our information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. This malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained.

Id.

34. The data purportedly affected includes payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards.

C. WAWA Understood the Value of Data Security

35. Like any merchant that handles payment cards and other sensitive data, WAWA was required to maintain the security and confidentiality of Private Information and protect it from unauthorized disclosure.

36. The Payment Card Industry Data Security Standards ("PCI DSS") are a list of twelve information security requirements promulgated by the Payment Card Industry Security Standards Council. They apply to all organizations and environments where cardholder data is stored, processed, or transmitted and require organizations to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks and ensure the maintenance of information security policies.

In addition, the PCI DSS prohibits WAWA from retaining certain customer data. Specifically, the PCI DSS 2.0 requires merchants to adhere to the following rules:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel

37. WAWA was at all times fully cognizant of its data protection obligations in light of the existing web of regulations requiring it to take affirmative steps to protect the sensitive financial information entrusted to it by consumers and the institutions that participate in and administer payment card processing systems.

38. Despite this, WAWA's treatment of the sensitive Private Information entrusted to it by its customers and the Plaintiff fell woefully short of its legal duties and obligations. WAWA failed to ensure that access to its data systems was reasonably guarded and protected and failed to acknowledge numerous warning signs and properly utilize its own security systems that were put in place to detect and deter this exact type of attack.

39. At the time of the breach, WAWA had specific notice of the potential threat of a data breach, and of the potential risks posed to the company and to the Plaintiff and the Class if it failed to adequately protect its systems.

40. WAWA's awareness of the importance of data security was bolstered in part by its observation of numerous other well-publicized data breaches involving major corporations being targeted for consumer information.

41. Other notable targets of large-scale data breaches include Yahoo (2013, more than three billion user accounts), Target Stores (2013), The Home Depot (2014), JP Morgan Chase (2014, 76 million American households and 7 million small businesses), Anthem (2015, nearly 80 million current and former plan members), Experian (2015, more than 15 million people's information), and most recently Equifax (2017, largest breach yet, exposing more than half the countries' personal and financial information) and Capital One (2019, exposing 100 million accounts).

42. Unfortunately, WAWA did not view these breaches as cautionary tales, but rather as another avenue to profit from businesses and consumers concerned with fraud.

D. The Impact of the WAWA Data Breach is Significant

43. There is no doubt that data breaches put consumers at an increased risk of fraud and identify theft. Private Information is a valuable commodity to identity thieves. Once information has been compromised, it often exists on the black-market for years.

44. As a direct and proximate result of WAWA's conduct, Plaintiff and class members are at an increased risk of harm from fraud and identity theft, and have suffered or will suffer actual injury as a direct result of the Data Breach. Injuries that have and will be incurred include: fraudulent charges, loss of use of and access to their account funds and costs associated with that

such as paying late or declined payment fees, damage to credit, out-of-pocket costs such as purchasing credit monitoring and identity theft prevention, the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

45. In addition, Plaintiff and class members have an interest in ensuring that their Private Information is protected from further breaches through security measures and safeguards.

46. WAWA's completely avoidable Data Breach inflicted significant financial damage upon the Plaintiff and the class, who must act immediately to mitigate potentially present fraud, while simultaneously taking steps to prevent future fraud and while continuing to meet the demands and needs of their financial lives.

47. The costs suffered by the Plaintiff and the class as a result of WAWA's data breach, measured in dollars as well as anxiety, emotional distress, and loss of privacy, will continue to mount.

COUNT ONE
VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681, *et seq.*

48. Plaintiff repeats and realleges Paragraphs 1-47 as if fully alleged herein.

49. Each time that WAWA accepts payment via payment card, it obtains, reviews, and uses a "consumer report," as that term is defined in 15 U.S.C § 1681a(d), about the person or entity by or for whom the payment was made.

50. WAWA is required by 15 U.S.C. §§ 1681b, 1681n, and 1681o to refrain from obtaining, disclosing or using consumer reports under false pretenses, and without proper authorization from the person or entity who is the subject of the report.

51. The furnishing of a consumer report is only permitted in specific instances. 15 U.S.C. §§ 1681b(a). Disclosing, or allowing consumer reports to be disclosed, is not allowed pursuant to FCRA, and thus is a violation of federal law.

52. Once obtained, WAWA has a mandatory duty to maintain and protect the use of consumer reports for permissible purposes only. 15 U.S.C. § 1681b(f). That includes instances where, but for actions taken or not taken by WAWA in data protection, the use of unlawful consumer reports obtained would not have occurred.

53. Despite these clear and unambiguous requirements of the FCRA, WAWA's actions and inactions have caused and will cause consumer reports regarding consumers to be obtained without their knowledge or consent in order to potentially open new, unauthorized accounts, in violation of FCRA.

54. Further, reports that were obtained in relation to the payments made may have been part of the collection of data that was exfiltrated in the data breach. Accordingly, WAWA failed to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

55. WAWA failed to maintain reasonable procedures designed to limit the furnishing of class members' consumer reports to permitted purposes, and/or failed to take adequate security measures that would prevent disclosure of class members' consumer reports to unauthorized entities or hackers.

56. As a direct and proximate result of WAWA's actions and failures to act described herein, and utter failure to take adequate and reasonable measures to ensure its data systems were protected, WAWA offered, provided, and furnished Plaintiff's and class members' consumer reports to unauthorized third parties.

57. Pursuant to 15 U.S.C. §§ 1681n and 1681o, WAWA is liable for negligently and willfully violating FCRA by accessing the consumer reports without a permissible purpose or authorization under FCRA.

COUNT TWO
NEGLIGENCE

58. Plaintiff repeats and realleges Paragraphs 1-57 as if fully alleged herein.

59. WAWA owed a duty to the Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, securing, and deleting the Private Information of customers.

60. WAWA owed a duty to the Plaintiff and the Class to provide security, at a minimum, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Private Information of customers.

61. WAWA owed a duty of care to the Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices. WAWA solicited, gathered, and stored the sensitive data provided by the Plaintiff and the Class. WAWA knew it inadequately safeguarded this information on its computer systems and that hackers would attempt to access this valuable data without authorization. WAWA knew that a breach of its systems would inflict damages upon the class, and WAWA was therefore charged with a duty to adequately protect this critically sensitive information.

62. WAWA maintained a special relationship with the Class. The Class entrusted WAWA with Private Information on the premise that it would safeguard this information, and WAWA was in a position to protect against the harm suffered by the class as a result of the Data Breach.

63. In light of its special relationship, WAWA knew, or should have known, of the risks inherent in collecting and storing the Private Information and the importance of providing adequate security of that information.

64. WAWA's own conduct also created a foreseeable risk of harm. Its misconduct included, but was not limited to, it not following broadly accepted security practices and not complying with industry standards for the safekeeping and maintenance of Private Information.

65. WAWA breached the duties it owed by failing to exercise reasonable care and implement adequate security protocols including protocols required by industry rules—sufficient to protect the Private Information at issue.

66. WAWA breached the duties it owed by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

67. WAWA breached the duties it owed by failing to properly maintain the sensitive Private Information. Given the risk involved and the amount of data at issue, WAWA's breach of its duty was entirely unreasonable.

68. WAWA, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and class members the fact that their Private Information within its possession might have been compromised and precisely the type of information compromised.

69. WAWA also knew that the Plaintiff and the Class were foreseeable victims of a data breach of its systems because of specific laws, regulations, and guidelines requiring it to reasonably safeguard sensitive information or be held liable in the event of a data breach.

70. As a direct and proximate result of WAWA's negligent conduct, the Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

71. In failing to secure Plaintiff's and class members' Private Information and promptly and specifically notifying them of the Data Breach, WAWA is guilty of oppression, fraud, or malice in that it acted or failed to act with a willful and conscious disregard of Plaintiff's and class members' rights. In addition to seeking actual damages, Plaintiff seeks punitive damages on behalf of herself and the Class.

72. Plaintiff also seeks injunctive relief on behalf of the Class compelling WAWA to implement appropriate data safeguarding methods and provide detailed and specific disclosure of the type(s) of information that have been compromised.

COUNT THREE
NEGLIGENT MISREPRESENTATION

73. Plaintiff repeats and realleges Paragraphs 1-72 as if fully alleged herein.

74. Through its privacy policies and other actions and representations, WAWA misrepresented to the Plaintiff and the Class that it possessed and maintained adequate data security measures and systems that were sufficient to protect Private Information.

75. WAWA further misrepresented that it would secure and protect Private Information by agreeing to comply with both Card Operating Regulations and the PCI DSS.

76. WAWA knew or should have known that it was not in compliance with the representations made in its privacy policies and the requirements of Card Operating Regulations and the PCI DSS.

77. WAWA knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to the Plaintiff and the Class.

78. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to the Plaintiff and the Class.

79. WAWA also failed to exercise reasonable care when it failed to timely communicate information concerning the Data Breach that it knew, or should have known, compromised the Private Information of customers.

80. Further, WAWA failed to adequately, timely and specifically communicate the occurrence of the Data Breach in a way that could inform and protect customers.

81. Plaintiff and the Class relied upon these misrepresentations and omissions to their detriment.

82. As a direct and proximate result of WAWA's negligent misrepresentations and omissions, Plaintiff and the Class have suffered and will continue to suffer injury and are entitled to damages in an amount to be proven at trial.

COUNT FOUR
DECLARATORY RELIEF

83. Plaintiff repeats and reallege Paragraphs 1-82 as if fully alleged herein.

84. 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, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

85. An actual controversy has arisen in the wake of the WAWA Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether WAWA is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information. Plaintiff alleges that WAWA's data security measures remain inadequate. WAWA denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the

compromise of her Private Information and remains at imminent risk that further compromises of Private Information will occur in the future.

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

a. WAWA continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. WAWA continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

87. The Court also should issue corresponding prospective injunctive relief requiring WAWA to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information and to adequately disclose information regarding the Data Breach.

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

89. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to WAWA if an injunction is issued. Among other things, if another massive data breach occurs at WAWA, Plaintiff will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to WAWA of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and WAWA has a pre-existing legal obligation to employ such measures.

90. 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 at WAWA, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of herself and the Class, respectfully requests that the Court enter judgment in her favor as follows:

a. certifying the class under Fed. R. Civ. P. 23 and appointing Plaintiff and her counsel to represent the class pursuant to Fed. R. Civ. P. 23(g);

b. awarding Plaintiff and the Class monetary damages as allowable by law;

c. awarding Plaintiff and the Class appropriate equitable relief;

d. awarding Plaintiff and the Class pre-judgment and post judgment interest;

e. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law; and

f. awarding all such further relief as allowable by law.

JURY TRIAL DEMANDED

Plaintiff, on behalf of herself and the Class, demands a trial by jury on all issues so triable.

Richard M. Golomb, Esquire
Kenneth J. Grunfeld, Esquire
GOLOMB & HONIK, P.C.
1835 Market Street, Suite 2900
Philadelphia, PA 19103
Phone: (215) 985-9177
Fax: (215) 985-4169

Attorneys for Plaintiffs and the Class

Dated: **December 20, 2019**