

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

EDWARD D. HOZZA, III, individually
and on behalf of himself and all other
persons similarly situated,
Plaintiff,

vs.

PRIMOHOAGIES FRANCHISING,
INC. d/b/a PRIMOHOAGIES,
Defendant.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff, Edward D. Hozza, III (“Plaintiff”), by and through his undersigned counsel, brings this class action lawsuit against Defendant PrimoHoagies Franchising, Inc. d/b/a PrimoHoagies (“Defendant” or “PrimoHoagies”), on behalf of himself and all others similarly situated, and alleges, based upon information and belief and the investigation of counsel as follows:

INTRODUCTION

1. Plaintiff brings this Action on behalf of a class of persons harmed as a result of PrimoHoagies’ failure to safeguard and protect its customers’ highly sensitive and personal payment card information, including, but not limited to names, addresses, payment card numbers, expiration dates, and security codes (“payment card information”), used on PrimoHoagies’ online payment platform.
2. On April 17, 2020, PrimoHoagies issued a “Customer Notice of Data

Security Incident”¹ on its website—disclosing for the first time that it discovered malware installed on its online payment platform on February 18, 2020, and that customer payment card information may have been affected (hereinafter referred to as “the data breach”). Unauthorized third parties used this malware to steal customers’ payment card information, including names, addresses, payment card numbers, expiration dates, and security codes, between July 15, 2019 and February 18, 2020 (the “relevant period”).

3. Plaintiff Hozza made numerous purchases using PrimoHoagies’ online payment platform with his credit card during the relevant period. As a result, Plaintiff’s payment card information was compromised by the malware infecting PrimoHoagies’ online payment platform. For example, after using PrimoHoagies’ online payment platform with his credit card during the relevant period, Plaintiff experienced fraudulent purchases on his credit card. Plaintiff’s credit card company contacted him about the fraud and issued Plaintiff a new card in September 2019

4. On April 17, 2020, Plaintiff received an email directly from PrimoHoagies indicating that his “payment card information may have been affected” by the data breach.

¹ Customer Notice of Data Security Incident, *available at* <https://www.primohoagies.com/orders/important-privacy-notice.php> (April 23, 2020).

5. Mitigating the actual and potential impact of the data breach will require Plaintiff, and other Class members, to undertake expensive and time-consuming efforts, including placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

6. Furthermore, Plaintiff and Class members will be required to purchase credit and identity monitoring services to alert them to potential misappropriation of their identity and to combat risk of further identity theft. At a minimum, Plaintiff and Class members have suffered compensable damages because they will be forced to incur the cost of a monitoring service which is a reasonable and necessary step to prevent and mitigate future loss.

THE PARTIES

7. Plaintiff, Edward D. Hozza, III (“Plaintiff”), is a resident of Lehigh County, Pennsylvania.

8. Defendant, PrimoHoagies Franchising, Inc. d/b/a PrimoHoagies (“PrimoHoagies”), is a Delaware corporation with its principal place of business located at 610 Ryan Avenue, Westville, New Jersey, 08093.

9. Defendant PrimoHoagies is the parent franchisor of a chain of casual sandwich restaurants by the same name “PrimoHoagies.” There are approximately

83 PrimoHoagies franchised restaurants located in eight (8) states—New Jersey, Pennsylvania, Delaware, Maryland, Virginia, South Carolina, Georgia, and Florida.

JURISDICTION AND VENUE

10. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 Class members, and at least one Class member is a citizen of a state different from the Defendant.

11. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

12. This Court has general personal jurisdiction over the Defendant. Defendant maintains their principal place of business in Westville, New Jersey and therefore is at home in this District.

13. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant’s principal place of business is located in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff’s claims occurred in this District.

FACTUAL ALLEGATIONS

A. The PrimoHoagies Data Breach

14. PrimoHoagies operates a casual restaurant chain specializing in Italian sandwiches.

15. PrimoHoagies operates and manages an e-commerce online payment platform on its website allowing customers to place orders for pickup or delivery from a PrimoHoagies restaurant location.

16. On April 17, 2020, PrimoHoagies issued a “Customer Notice of Data Security Incident”² on its website disclosing for the first time that it discovered malware installed on its online payment platform on February 18, 2020, and that customer payment card information may have been affected.

17. The notice further disclosed that an internal investigation determined unauthorized third parties used this malware to steal payment card information, including names, addresses, payment card numbers, expiration dates, and security codes.

18. According to PrimoHoagies, the malware affected payment cards used by customers for online purchases between July 15, 2019 and February 18, 2020.

19. On April 17, 2020, PrimoHoagies sent an email containing a link to this Notice to affected customers whose data had been compromised, including

² Customer Notice of Data Security Incident.

Plaintiff.

20. Plaintiff used his credit card to make purchases on PrimoHoagies' online payment platform during the relevant period.

21. As such, Plaintiff's payment card information was routed through PrimoHoagies' online payment system and intercepted by the malware.

22. After using his credit card to make purchases on PrimoHoagies' online payment platform during the relevant period, Plaintiff incurred fraudulent charges on his credit card. As a result of these fraudulent charges, in September 2019, Plaintiff's credit card company issued him a new credit card.

B. The Data Breach Caused Harm to Plaintiff and Class Members

23. Payment card data such as credit or debit card information is highly valuable because criminals can use this stolen information to commit a variety of financial crimes. As a result, credit and debit card information that is stolen from payment card processing systems, online payment platforms, and other locations are frequently sold on the "dark web." This information can also be used to clone credit and/or debit cards facilitating fraudulent transactions.

24. Despite well-publicized litigation and frequent public announcements of data breaches, PrimoHoagies failed to implement and maintain security procedures and practices necessary to protect Plaintiff's and Class members' payment card information.

25. Federal and state governments have established security standards and issued recommendations intended to prevent data breaches and the resulting harm to consumers and financial institutions. For example, the Federal Trade Commission (“FTC”) has issued specific guidance for businesses highlighting the importance of data security practices.³

26. Under the FTC guidelines, businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to identify breaches as soon as possible, monitor all incoming traffic for activity indicating an attack on their systems, watch for the transmission of large amounts of data, and develop a response plan in the event of a breach.

27. The FTC also recommends that companies delete cardholder information that is no longer needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security

³ FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Oct. 2016), *available at* <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

measures.

28. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 (2006). *See, e.g., Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3d Cir. 2015); *In re BJ’s Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

29. PrimoHoagies’ failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer payment card information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

30. Additionally, the Payment Card Industry Security Standards Council has promulgated a list of twelve information security requirements, commonly known as the Payment Card Industry Data Security Standard (“PCI DSS”).

31. The PCI DSS is the global data security standard adopted by all major payment card brands and is applicable to all entities that process, store, or transmit cardholder data and/or sensitive authentication data.

32. Under the PCI DSS, merchants, such as PrimoHoagies, are required 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.

33. The twelve requirements of the PCI DSS are:⁴

- Install and maintain a firewall configuration to protect cardholder data;
- Do not use vendor-supplied defaults for system passwords and other security parameters;
- Protect stored cardholder data;
- Encrypt transmission of cardholder data across open, public networks;
- Protect all systems against malware and regularly update anti-virus software or programs;
- Develop and maintain secure systems and applications;
- Restrict access to cardholder data by business need to know;
- Identify and authenticate access to system components;
- Restrict physical access to cardholder data;
- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes; and
- Maintain a policy that addresses information security for all personnel.

34. PrimoHoagies was at all times fully aware of its obligation to protect

⁴ Payment Card Industry Security Standards Council, “PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1,” at p. 9, *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

the personal and financial data of its customers because of its participation in payment card processing networks and the large volume of card-based transactions PrimoHoagies processes through its online payment platform.

35. PrimoHoagies, as a business that operates in multiple states, was also fully aware of its obligation to protect customers' payment card information in accordance with state and federal law and industry guidelines.

36. PrimoHoagies knew of the significant repercussions that Plaintiff and the Class would suffer if it failed to do so, as the harm caused by identity theft is widely disseminated in the news media and industry publications.

37. Despite understanding the consequences of maintaining inadequate data security, PrimoHoagies failed to maintain appropriate security measures to protect and secure customers' payment card information.

38. In the case of a data breach, merely reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."⁵

39. A victim whose payment card information has been stolen or

⁵ See Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims of Identity Theft, 2012*, U.S. Department of Justice, Bureau of Justice Statistics (Dec. 2013), at 1.

compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose payment card information has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

40. According to the BJS, an estimated 16.6 million people were victims of one or more incidents of identity theft in 2012. Among identity theft victims, existing bank or credit card accounts were the most common types of misused information.⁶

41. Due to PrimoHoagies' failure to promptly identify the data breach and alert customers, Plaintiff and Class members were unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their payment card information without being able to take necessary precautions to prevent imminent harm.

42. As a result of the data breach, Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

43. Plaintiff and Class members are also subject to a higher risk of cyber-attacks, including "phishing" where hackers exploit information they have already

⁶ *Id.*

obtained to send deceptive emails to convince the recipient to take action (*e.g.*, click on an embedded hyper-link or download software), that would reveal additional personal and financial information.

44. Plaintiff and Class members are presently incurring and will continue to incur such damages in addition to fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the bank or credit card companies.

45. The exposure of Plaintiff's and Class members' payment card information to malware was a direct and proximate result of PrimoHoagies' failure to properly safeguard and protect Plaintiff's and Class members' payment card information from unauthorized access, use, and disclosure. PrimoHoagies failed to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' payment card information in order to protect it against reasonably foreseeable threats to the security of such information.

46. Plaintiff's and Class members' payment card information is highly valuable, private and sensitive in nature and was inadequately protected by PrimoHoagies.

47. As one of the east coast's leading casual sandwich chains with over 83

locations, PrimoHoagies had the sophisticated financial and technical resources to prevent such a malware breach. However, PrimoHoagies has neglected to adequately invest in data security, despite the growing number of data intrusions and several years of well-publicized data breaches.

48. Had PrimoHoagies remedied the deficiencies in its payment processing and security systems, followed industry guidelines, and adopted measures recommended by the FTC and experts in the field, PrimoHoagies would have prevented intrusion into its payment processing and security systems and, ultimately, the theft of Plaintiff's and Class members' payment card information.

49. As a direct and proximate result of PrimoHoagies wrongful actions and inaction, Plaintiff and Class members have been placed at an immediate and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the PrimoHoagies data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

50. PrimoHoagies' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' payment card information, causing them to suffer,

and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. The improper disclosure, compromising and theft of their payment card information;
- b. Unauthorized charges on their debit and credit card accounts;
- c. The imminent and impending injury flowing from potential fraud and identity theft posed by their payment card information being placed in the hands of unauthorized parties and misused via the sale of Plaintiff's and Class members' payment card information on the internet black market and dark web;
- d. The untimely and inadequate notification of the data breach;
- e. Loss of privacy;
- f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;
- g. Loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and
- h. The loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the data breach.

51. PrimoHoagies has failed to offer any form of credit monitoring or other recourse as a result of the data breach. As previously alleged, Plaintiff's and Class Member's payment card information may exist on the dark web for months, or even years, after the initial breach. With no form of insurance or other protection, Plaintiff and Class members remain unprotected from the real and long-term threats of having their payment card information exposed. Plaintiff and Class members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

CLASS ACTION ALLEGATIONS

52. Plaintiff, Edward D. Hozza, III, brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and all others similarly situated, as representative of the following Class:

All persons residing in the United States whose payment card information was accessed, compromised, or stolen as a result of the data breach disclosed by Defendant on April 17, 2020.

53. The aforementioned Class is referred to herein as the "Class."

54. Excluded from the Class are affiliates, predecessors, successors, officers, directors, agents, servants, or employees of Defendant's, and the immediate family members of such persons. Also excluded are any trial judge who may preside over this action and their law clerks, court personnel and their family members, and any juror assigned to this action.

55. Plaintiff reserves the right to amend the Class definition if discovery and/or further investigation reveal that it should be modified.

56. The members of the Class are so numerous that the joinder of all members of the Class in a single action is impractical. While the exact number of Class members is unknown to Plaintiff at this time, PrimoHoagies has acknowledged that its customers' payment card information was compromised for over nine months. Therefore, it stands to reason that the number of Class members is likely in the millions. The Class members are readily identifiable from information and records in Defendant's possession, custody, or control, such as transaction records and purchases.

57. There are common questions of law and fact to the Class members, which predominate over any questions affecting only individual Class members.

These common questions of law and fact include, without limitation:

- a. Whether Defendant owed a duty to Plaintiff and Class members to safeguard and protect the security of their payment card information;
- b. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff's and Class members' payment card information; and
- c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class members' payment card information from unauthorized capture, dissemination and misuse.

58. Plaintiff's claims are typical of those of other Class members because Plaintiff's payment card information, like that of every other Class member, was

misused and improperly disclosed by Defendant.

59. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained competent counsel experienced in litigating complex class actions, including consumer class actions. Plaintiff intends to prosecute this action vigorously. Plaintiff's claims are typical of the claims of all of the other Class members, and Plaintiff has the same non-conflicting interests as the other Class members. Therefore, the interests of the Class members will be fairly and adequately represented by Plaintiff and his counsel.

60. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go unremedied.

CLAIMS FOR RELIEF

COUNT I

(Negligence)

61. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

62. PrimoHoagies owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their payment card information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

63. This duty included, among other things, designing, maintaining, and testing PrimoHoagies' security systems to ensure that Plaintiff's and Class members' payment card information was adequately secured and protected in accordance with federal, state and industry guidelines.

64. PrimoHoagies further had a duty to implement processes that would detect a breach of their security system in a timely manner.

65. PrimoHoagies also had a duty to timely disclose to Plaintiff and Class members that their payment card information had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that, among other things, Plaintiff and Class members could take appropriate measures to cancel or

change their debit or credit cards, to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts, and take all other appropriate precautions.

66. PrimoHoagies breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' payment card information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, allowing unauthorized access to Plaintiff's and Class members' payment card information, and failing to recognize the breach in a timely manner.

67. PrimoHoagies breached its duty to timely disclose that Plaintiff's and Class members' payment card information had been, or was reasonably believed to have been, stolen or compromised.

68. PrimoHoagies' failure to comply with industry regulations and the delay between the date of intrusion and the date PrimoHoagies informed customers of the data breach further evidence PrimoHoagies' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' payment card information.

69. But for PrimoHoagies' wrongful and negligent breach of its duties owed to Plaintiff and Class members, their payment card information would not have been compromised, stolen, and viewed by unauthorized persons.

70. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of PrimoHoagies' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' payment card information. PrimoHoagies knew or should have known that their systems and technologies for processing and securing Plaintiff's and Class members' payment card information had security vulnerabilities susceptible to malware.

71. As a result of PrimoHoagies' negligence, Plaintiff and Class members incurred damages including, but not limited to, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of PrimoHoagies' security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit and debit cards of PrimoHoagies' customers by identity thieves who wrongfully gained access to Plaintiff's and Class members' payment card information.

COUNT II

(Negligence *Per Se*)

72. Plaintiff repeats, realleges, and incorporates by reference the

allegations contained in each and every paragraph above, as though fully stated herein.

73. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the failure to use reasonable measures to protect payment card information.

74. PrimoHoagies violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff’s and Class members’ payment card information and by failing to comply with industry standards. PrimoHoagies’ conduct was particularly unreasonable given the amount of payment card information it processed and the foreseeable consequences of a data breach.

75. PrimoHoagies’ violation of Section 5 of the FTC Act constitutes negligence *per se*.

76. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

77. Moreover, the harm that has occurred is the type of harm the FTC Act 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.

78. As a direct and proximate result of PrimoHoagies’ negligence,

Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III

(Breach of Implied Contract)

79. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

80. When Plaintiff and Class members paid money and provided their payment card information to PrimoHoagies in exchange for goods and services, they entered into implied contracts with PrimoHoagies pursuant to which PrimoHoagies agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

81. PrimoHoagies solicited and invited prospective consumers such as Plaintiff and Class members to provide their payment card information as part of its regular business practices by using their credit and/or debit cards. Plaintiff and Class members accepted PrimoHoagies' offers and provided their payment card information to PrimoHoagies.

82. In entering into such implied contracts, Plaintiff and Class members reasonably assumed that PrimoHoagies' data security practices and policies were

reasonable and consistent with industry standards, and that PrimoHoagies would use part of the funds received from Plaintiff and Class members to pay for adequate and reasonable data security practices.

83. Plaintiff and Class members would not have entrusted their payment card information to PrimoHoagies in the absence of the implied contract between them and PrimoHoagies to keep the information secure.

84. Plaintiff and Class members fully performed their obligations under the implied contracts with PrimoHoagies by paying for goods and services.

85. PrimoHoagies breached their implied contracts with Plaintiff and Class members by failing to safeguard and protect their payment card information and by failing to provide timely and accurate notice that their payment card information was compromised as a result of the Data breach.

86. As a direct and proximate result of PrimoHoagies' breaches of their implied contracts, Plaintiff and Class members sustained actual losses and damages, including, but not limited to, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of PrimoHoagies' security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic

payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit and debit cards of PrimoHoagies' customers by identity thieves who wrongfully gained access to Plaintiff's and Class members' payment card information.

COUNT IV

(For Violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law)

(73 P.S. § 201-1, *et seq.*)

87. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

88. As a consumer of PrimoHoagies' services, Plaintiff is authorized to bring a private action under Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"). 73 P.S. § 201-9.2.

89. Plaintiff is a "person" within the meaning of 73 P.S. § 201-2(2).

90. Plaintiff and Class members provided their payment card information to PrimoHoagies pursuant to transactions in "trade" and "commerce" as meant by 73 P.S. §201-2(3), for personal, family, and/or household purposes.

91. The UTPCPL prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce[.]" 73 P.S. § 201-3.

92. This Count is brought for PrimoHoagies' unfair and deceptive

conduct, including PrimoHoagies' unlawful and unfair and deceptive acts and practices, which "creat[ed] a likelihood of confusion or of misunderstanding" for Plaintiff and Class members as meant by 73 P.S. § 201-2(4)(xxi).

93. PrimoHoagies engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale and advertisement of the goods purchased by Plaintiff and the Class in violation of 73 P.S. § 201-3, including but not limited to the following:

- a. PrimoHoagies failed to enact adequate privacy and security measures to protect Plaintiff's and Class members' payment card information from unauthorized disclosure, release, data breaches, malware, and theft, which was a direct and proximate cause of the data breach;
- b. PrimoHoagies negligently represented that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' payment card information from unauthorized disclosure, release, data breaches, malware and theft was unfair and deceptive given the inadequacy of its privacy and security protections; and
- c. PrimoHoagies' negligence in failing to disclose the material fact of the inadequacy of its privacy and security protections for Plaintiff and Class members was unfair and deceptive.

94. The above unfair and deceptive acts and practices by PrimoHoagies were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

95. PrimoHoagies knew or should have known that their computer

systems and data security practices were inadequate to safeguard Plaintiff's and Class members' payment card information and that the risk of a data breach or theft was highly likely. PrimoHoagies' actions in engaging in the above-named deceptive acts and practices were negligent, knowing, and reckless with respect to the rights of members of the Class.

96. Plaintiff and Class members relied on PrimoHoagies' unfair and deceptive acts and practices when they paid money in exchange for goods and services and provided their payment card information through PrimoHoagies' online payment platform.

97. Plaintiff and Class members relied on PrimoHoagies to safeguard and protect their payment card information and to timely and accurately notify them if their data had been breached and compromised.

98. Plaintiff and Class members seek all available relief under the UTPCPL, 73 P.S. § 201-1, *et seq.*

COUNT V

(For Violation of New Jersey's Consumer Fraud Act)

(N.J.S.A. § 56:8-2, *et seq.*)

99. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

100. The New Jersey Consumer Fraud Act (the “NJCFA”), N.J.S.A. § 56:8-1, *et seq.*, prohibits the act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression or omission, in connection with the sale or advertisement of any merchandise. The NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J.S.A. § 56:8-2.

101. Plaintiff Hozza, Defendant PrimoHoagies, and class Members are “persons” within the meaning of N.J.S.A. § 56:8-1(d).

102. PrimoHoagies sells “merchandise,” as defined by N.J.S.A. § 56:8-1, by offering sandwiches, foodstuffs, and services to the public.

103. PrimoHoagies, which is headquartered in New Jersey, engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of convenience store goods and services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

- a. PrimoHoagies failed to enact adequate privacy and security measures to protect Plaintiff’s and Class members’ payment card information from unauthorized disclosure, release, data breaches, malware, and theft, which was a direct and proximate cause of the data breach;
- b. PrimoHoagies negligently represented that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff’s and Class members’ payment card information from unauthorized disclosure,

release, data breaches, malware and theft was unfair and deceptive given the inadequacy of its privacy and security protections;

- c. PrimoHoagies' negligence in failing to disclose the material fact of the inadequacy of its privacy and security protections for Plaintiff and Class members was unfair and deceptive;
- d. PrimoHoagies' unconscionable and deceptive acts and practices with respect to the sale of food items and services by failing to adequately monitor and audit the data security systems of its vendors and business associates and failing to maintain the privacy and security of Plaintiff and Class members in violation of duties imposed by and public policies reflected in the FTC Act; and
- e. PrimoHoagies' unconscionable and deceptive acts and practices in failing to disclose the data breach to Plaintiff and Class members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163.

104. The above unlawful and deceptive acts and practices by PrimoHoagies were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

105. PrimoHoagies knew or should have known that its data security practices were inadequate to safeguard Plaintiff's and Class members' payment card information and that the risk of a data breach was highly likely.

PrimoHoagies' actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class members.

106. Plaintiff's and Class members reasonably expected that PrimoHoagies would protect their payment card information and reasonably expected that PrimoHoagies would provide truthful statements on its website and privacy policies, and that it would be safe to provide PrimoHoagies with their information. These representations and affirmations of fact made by PrimoHoagies, and the facts it concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not to provide their information to PrimoHoagies. PrimoHoagies, moreover, intended for consumers, including Plaintiff and Class members, to rely on these material facts.

107. As a direct and proximate result of PrimoHoagies' unconscionable and deceptive acts and practices, Plaintiff and Class members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their payment card information.

108. Plaintiff and Class members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

109. Pursuant to N.J.S.A. § 56:8-20, this Complaint will be served upon the New Jersey Attorney General.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, Edward D. Hozza, III, individually and on behalf of the Class, respectfully requests that the Court:

- A. Certify the Class pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class members;
- B. Designate Plaintiff as representative of the Class and the undersigned counsel, Lowey Dannenberg, P.C. as Class Counsel;
- C. Award Plaintiff and the Class compensatory damages in an amount to be determined by the Court and treble and punitive damages to punish Defendant's egregious conduct as described herein, and to deter Defendant and others from engaging in similar conduct;
- D. Award Plaintiff and the Class injunctive relief, as permitted by law or equity, including enjoining Defendant from continuing the unlawful practices set forth herein, ordering Defendant to fully disclose the extent and nature of the security breach and theft, and ordering Defendant to pay for not less than three years of identity theft and credit card monitoring services for Plaintiff and the Class;
- E. Award Plaintiff and the Class statutory interest and penalties;
- F. Award Plaintiff and the Class their costs, prejudgment and post judgment interest, and attorneys' fees; and
- G. Grant such other relief that the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury as to all issues stated herein, and all issues so triable.

Dated: April 23, 2020
West Conshohocken, PA

Respectfully submitted,

By: /s/ Anthony M. Christina
Anthony M. Christina (NJ ID # 196262016)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Email: achristina@lowey.com

Christian Levis (NJ ID # 021492012;
D.N.J. *General Admission* forthcoming)
Amanda Fiorilla (NJ ID # 317282020;
D.N.J. *General Admission* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Email: clevis@lowey.com
afiorilla@lowey.com

Attorneys for Plaintiff Edward D. Hozza, III