UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA

Jonathan Torres, Christine Jackson, Donald Jackson, Ashley McConnell, Roxanne Gant, and Gerald Thomas, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

Wendy's International LLC,

Defendant.

Case No. 6:16-cv-210-PGB-DCI

SECOND AMENDED CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiffs Jonathan Torres, Christine Jackson, and Donald Jackson, Ashley McConnell, Roxanne Gant, and Gerald Thomas, by and through their undersigned counsel, bring this Second Amended Class Action Complaint against Wendy's International LLC, on behalf of themselves and all others similarly situated, and allege, upon personal knowledge as to their own actions, upon their counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Wendy's International LLC (referred to herein as "Wendy's" or "Defendant") for its failure to secure and safeguard its customers' credit and debit card numbers and other payment card data ("PCD"), and other personally identifiable information ("PII") which Wendy's collected at the time Plaintiffs made restaurant purchases at Wendy's (collectively, "Customer Data"), and for failing to provide timely, accurate and

adequate notice to Plaintiffs and other Class members that their Customer Data had been stolen and precisely what types of information were stolen.

2. On July 7, 2016, Wendy's finally revealed that customers at over 1,000 of its franchise restaurants—approximately 20% of its franchise locations—had their Customer Data stolen starting in the fall of 2015 and continuing through at least early June 2016 (the "Data Breach"). Just two months prior to this announcement, and five months into Wendy's investigation of the Data Breach, Wendy's stated that the Data Breach affected "less than 300" of its stores; now that estimate has more than tripled. Even in its, July 7 announcement, Wendy's noted that the investigation was still "ongoing."

3. Wendy's has yet to disclose the approximate number of customers whose Customer Data was appropriated by unauthorized third parties during the at least nine-month long Data Breach period; however, in the spring of 2015, it was estimated that Wendy's served approximately 50 million customers per month.[1]

4. Hackers installed malware designed to steal credit and debit card data on Wendy's point-of-sale ("POS") systems. Wendy's has indicated that cybercriminals gained access via a third-party vendor with access to Wendy's systems.

5. The Customer Data stolen as a result of the Data Breach includes cardholder names, credit/debit card numbers, expiration dates, cardholder verification values and service codes.

6. Wendy's could have prevented this Data Breach. Data breaches at other retail establishments in the last few years have been the result of malware installed on POS systems. While many retailers, banks and other companies have responded to recent breaches by adopting technology that helps makes transactions more secure, Wendy's did not.

[1] See, http://www.statista.com/statistics/230988/people-who-visited-wendys-usa/ (last visited July 24, 2016).

7. The Data Breach was the inevitable result of Wendy's inadequate approach to data security. The deficiencies in Wendy's data security were so significant that the malware installed by the hackers remained undetected and intact for months, and hackers were able to continue stealing Customer Data, even after Wendy's itself was aware of and began to disclose the existence of the breach.

8. Wendy's disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Customer Data.

9. On information and belief, the Customer Data of Plaintiffs and Class members was improperly handled and stored; was unencrypted; and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, the Customer Data of Plaintiffs and Class members was compromised and stolen. Moreover, as this same information remains stored in Wendy's computer systems, which Wendy's has shown an utter inability to safeguard, Plaintiffs and Class members have an interest in ensuring that their information is safe, and they should be entitled to seek injunctive and other equitable relief, including independent oversight of Wendy's security systems.

PARTIES

10. Plaintiff Jonathan Torres is a resident of the state of Florida. On January 3, 2016, Plaintiff Jonathan Torres visited a Wendy's restaurant in Orlando, Florida and purchased food items using his debit card issued by his credit union. Shortly thereafter, Mr. Torres was contacted by his credit union advising that his credit card number had been used to make a purchase at a

Sport's Authority in the amount of $200, and $377.74 at a Best Buy store. These transactions were not made or authorized by Mr. Torres, and were made even though he had physical possession of his credit card at the time these fraudulent transactions were made. Plaintiff completed paperwork to report the fraud to his credit union and reported the theft to local law enforcement.

11. Due to these fraudulent charges drawing money out of his account, Mr. Torres was without sufficient funds to pay his financial obligations. He was late paying his monthly child support and an additional child support obligation that was owed at the time because of his daughter's recent birthday. He was unable to pay his electric bill on time and was assessed a $3.00 late charge, which he paid.

12. Plaintiff Christine Jackson is a resident of the state of New York. On or about March 24, 2016, Mrs. Jackson visited a Wendy's restaurant in Miller Place, NY and purchased food items using her PayPal debit card. Wendy's website notes that this location was subject to the data breach, for more than six months, between approximately December 2, 2015 and June 8, 2016. Mrs. Jackson does not use her PayPal debit card frequently, and the majority of the debit card charges on her PayPal account during the relevant time period were charges placed on her husband's card (which bears its own card number). In April 2016, less than a month after visiting Wendy's, Mrs. Jackson's husband, Plaintiff Donald Jackson, received email alerts from PayPal advising the Jacksons that Mrs. Jackson's debit card number had been used to make three purchases at Area 516 Nightclub; those purchases amounted to $16, $13, and $31. Mr. Jackson was also alerted to an attempt to charge $377 to the Long Island Railroad on April 29, 2016. These transactions were not made or authorized by the Jacksons, and were made even though Mrs. Jackson had physical possession of her debit card at the time these fraudulent transactions

were made. The Jacksons have reported this theft to their debit card company. As a result of these fraudulent charges, Mrs. Jackson's debit card was cancelled on or about April 30, 2016, and she did not receive a replacement card until approximately May 10, 2016.

13. Plaintiff Donald Jackson is a resident of the state of New York. Mr. Jackson holds a joint PayPal debit account with his wife, Plaintiff Christine Jackson. As a result of the fraudulent charges on Mrs. Jackson's PayPal debit card number, Mr. Jackson's PayPal debit card (on the Jacksons' joint account) was cancelled on or about April 30, 2016 and he did not receive a replacement card until approximately May 10, 2016. Mr. Jackson uses his PayPal debit card for the vast majority of his expenses because the card offers 1% cash back. Because the Jacksons' debit cards were cancelled as a result of the Data Breach and subsequent fraudulent charges, the Jacksons had to use cash and other credit or debit cards while awaiting their replacement cards; accordingly, they lost the 1% cash back for those charges that would have otherwise been charged to their PayPal debit account. The Jacksons lost an estimated $7.88 in foregone cash back while awaiting their replacement cards. Mr. Jackson also spent time corresponding with PayPal regarding these fraudulent charges and replacement cards; updating account information for bills that were set up to be automatically paid with the Jacksons' PayPal account; and reviewing statements.

14. The fraudulent charges to the Jacksons' PayPal debit account were discovered while the Jacksons were on vacation and staying in a hotel held on the Jacksons' PayPal debit card. Consequently, the Jacksons spent time during their vacation to resolve the bill with the hotel and add a new credit card to the file, and faced embarrassment at having to remedy a non-working card with the hotel. Their vacation was further negatively impacted by their inability to access funds in their PayPal account. For example, the inability to access these funds prevented

them from making purchases they otherwise would have made and required them to cut short their vacation.

15. Plaintiff Ashley McConnell is a resident of the state of Tennessee. On or around January 20, 2016, she used her bank card for food purchases at the Wendy's on Wilma Rudolph Boulevard in Clarksville, Tennessee. Wendy's website notes that this location was subject to the data breach for six months between approximately January 13, 2016 and June 8, 2016. The day following her purchase at Wendy's, Plaintiff Ashley McConnell was alerted by her bank that her card had been used for a fraudulent transaction during the night in Indiana. This transaction was not made or authorized by Ms. McConnell, and was made even though she had physical possession of her credit card at the time the fraudulent charge was made. Due to the fraudulent activity, her bank closed the account and reissued a new payment card, leaving Ms. McConnell without access to her bank account for several days at a time during which her wages were deposited. During this time, she was prevented from making purchases that she would otherwise have made. As a result of the Data Breach, Ms. McConnell was required to spend time corresponding with her bank regarding the fraudulent charges, account closing and replacement card.

16. Plaintiff Roxanne Gant is a resident of the state of Texas. On or around April 6, 2016, she used her debit card for food purchases at the Wendy's at 243 Greens Road in Houston, Texas. Wendy's website notes that this location was subject to the data breach for more than six months between approximately December 2, 2015 and June 8, 2016. On or around May 7, 2016, the card company, Direct Express, sent her a letter advising of suspicious activity on her card and that temporary restrictions had been placed on her card as a result. When Ms. Gant called Direct Express she learned that six fraudulent charges had been made to her account, one of which had

transpired in Great Britain. These charges were not made or authorized by Ms. Gant, and were made even though she had physical possession of her credit card at the time the transactions occurred. Due to the fraudulent activity, Direct Express closed Ms. Gant's account, opened a new account and issued a new debit card to her. Ms. Gant did not receive the new debit card for approximately two weeks.

17. Direct Express partners with a program called Pay Perks. This program allows Direct Express customers to earn points that can be redeemed for cash prizes. One method of earning points is by using the debit card for financial transactions. Because Ms. Gant's debit card was cancelled as a result of the Data Breach and subsequent fraudulent charges, she had to use cash and other credit or debit cards while awaiting her replacement card; accordingly, she lost the Pay Perks points for those charges that would have otherwise been charged to her Direct Express debit account. Ms. Gant also spent time corresponding with Direct Express regarding the fraudulent charges, account closing and replacement card, and updating account information for bills that were set up to be automatically paid with the Direct Express card.

18. On or about April 15, 2016, Plaintiff Gant used a Kaiku pre-paid Visa card for food purchases at the same Wendy's located at 243 Greens Road in Houston, Texas. On or about June 10, 2016, this pre-paid Visa card was used fraudulently for a $2.33 charge with an additional $25.00 cash back with the purchase. These charges were not made or authorized by Ms. Gant, and were made even though she had physical possession of her credit card at the time the transactions occurred. As a result of this fraudulent activity, Ms. Gant was required to spend time corresponding with Kaiku cardholder services regarding the fraudulent charges, reversing of the charges, closing the account and having a replacement card issued.

19. Plaintiff Gerald Thomas is a resident of New Jersey. He used his credit card for food purchases at the Wendy's restaurant located at 35 U.S. Hwy 206 South on December 16, 2015, January 7, 2016, January 19, 2016, and February 1, 2016. Wendy's website notes that this location was subject to the data breach for six months between approximately December 2, 2015 and June 8, 2016. On the evening of April 3, 2016, just as he was set to leave on a business trip, Mr. Thomas received a fraud alert email from his bank. When he called his bank, Mr. Thomas learned that fraudulent charges had been made to his card even though he had physical possession of his credit card at the time the transactions occurred.

20. The bank wanted to close the credit card account and re-issue a new card, but Mr. Thomas had no other credit card to use for his upcoming business travel. Accordingly, the bank agreed to keep open the account while Mr. Thomas was traveling, but on the condition that certain restrictions were placed on the account. These restrictions required Mr. Thomas to call into the bank each time he needed to make a purchase. With every purchase, he would have to know the total amount of the transaction first, then call into the bank fraud department, and proceed to wait on hold while the transaction was approved. This burdensome process for each expense on his travel cost him time and caused much embarrassment. Prior to the fraudulent activity on his credit card, Mr. Thomas had invited a friend to have dinner with him during his trip. Because of the restrictions placed on his card, Mr. Thomas had to ask the friend to pay for dinner and then he subsequently repaid the friend once his account was restored without restrictions.

21. Once Mr. Thomas returned home, the bank closed his account and he waited approximately four days before receiving his replacement card. Mr. Thomas uses this credit card for all purchases because of the cash rewards it occurs. During his travel when the account

restrictions hindered his purchasing and during the time he was awaiting his replacement card, Mr. Thomas was prevented from making purchases that he otherwise would have made, thereby forgoing the cash back rewards that he normally would have earned.

22. Defendant Wendy's International LLC is an Ohio limited liability company, maintains its headquarters in Dublin, Ohio and is authorized to do business in this state.

23. Wendy's (NASDAQ: WEN) is the world's third largest quick-service hamburger company. As of January 3, 2016, there were 6,076 Wendy's restaurants in North America, 632 of which are operated by Wendy's with the remaining 5,444 operated by a total of 390 franchisees.[2]

JURISDICTION AND VENUE

24. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000, exclusive of interest and costs, and this is a class action in which more than two-thirds of the proposed plaintiff class, on the one hand, and Wendy's, on the other, are citizens of different states.

25. This Court has jurisdiction over Wendy's as it operates restaurants serving the public, and it is at one of the restaurants in this District that Plaintiff Torres made a purchase using his debit card which led to the damages that he suffered. Wendy's also advertises in a variety of media throughout the United States, including Florida and this District. Through its business operations in this District, Wendy's intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

[2] The Wendy's Company annual Form 10-K filed with the SEC on March 3, 2016, available at http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTEwNzkyMDUyJkRTRVE9MCZTRVE9MCZTUURFU0M9U0VDVElPTl9FTlRJUkUmc3Vic2lkPTU3 (last visited July 21, 2016).

26. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, Wendy's operates restaurants within this District, and Wendy's has caused harm to Class members residing in this District.

FACTUAL BACKGROUND

A. Wendy's and Its Customer Data Collection Practices

27. Wendy's derives its revenues from restaurant operations, management and franchise fees, and other revenues. In connection with its operations, Wendy's has acknowledged in its filings with the United States Securities and Exchange Commission the problems inherent with the collection of information from consumers. Specifically, it has stated:

> We rely on computer systems and information technology to run our business. Any material failure, interruption or security breach of our computer systems or information technology may result in adverse publicity and adversely affect the operation of our business and results of operations. We are significantly dependent upon our computer systems and information technology to properly conduct our business. A failure or interruption of computer systems or information technology could result in the loss of data, business interruptions or delays in business operations. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. A significant security breach of our computer systems or information technology could require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, and incur penalties or other costs that could adversely affect the operation of our business and results of operations.
>
> Failure to comply with laws, regulations and third-party contracts regarding the collection, maintenance and processing of information may result in adverse publicity and adversely affect the operation of our business and results of operations.
>
> We collect, maintain and process certain information about customers and employees. Our use and protection of this information is regulated by various laws and regulations, as well as by third-party contracts. If our systems or employees fail to comply with these laws, regulations or contract terms, it could

> require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, increase fees payable to third parties, and incur penalties or remediation and other costs that could adversely affect the operation of our business and results of operations. [3]

28. When consumers make purchases at Wendy's restaurants, they often pay for their purchases using credit or debit cards, and Wendy's collects PCD related to that card including the cardholder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards. Wendy's stores the PCD in its point-of-sale system and transmits this information to a third party for completion of the payment.

B. Stolen Customer Data Is Valuable to Hackers and Thieves

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

30. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[4]

31. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as

[3] The Wendy's Company annual Form 10-K filed with the SEC on February 27, 2014, available at http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTk0MjUxMjYmRFNFUT0xJlNFUT0xOSZTUURFU0M9U0VDVElPTl9QQUdFJmV4cD0mc3Vic2lkPTU3 (last visited July 22, 2016).

[4] Verizon 2014 PCI Compliance Report, available at http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited July 22, 2016).

retailers, Wendy's approach to maintaining the privacy of Plaintiffs' and Class members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

C. Wendy's POS Systems Were Outdated and Vulnerable to Attack

32. In 2012, Wendy's announced plans to implement a single, consistent POS platform for the entire Wendy's restaurant system in the United States and Canada.[5] The transition was necessary, according to Wendy's, because its POS systems were outdated.[6]

33. Wendy's never converted to a single POS system, instead allowing franchisees to choose the lowest-priced POS system that fit the criteria required by Wendy's. Different POS systems have different security protocols with varying levels of strength. Having multiple POS systems throughout the chain can make it more difficult to prevent, investigate, and detect a security breach because of the different security protocols.

34. POS systems are typically run by a third-party vendor. Having multiple POS systems means multiple vendors have access to company systems and Customer Data.

35. Wendy's has said that the Data Breach did not affect the "Aloha" POS system that it set about to implement chain-wide in 2012, had already installed in all company-operated restaurants, and now hopes to install at all restaurants (including franchise locations) by the end of 2016.[7]

---

[5] Compl. at ¶16, *Wendy's International, LLC v. DavCo Restaurants, LLC*, No. 14-cv-013382 (Ct. Comm. Pls., Franklin City, Ohio) available at http://www.bluemaumau.org/sites/default/files/WEN%20v.%20DAVCO,%20Dec%2022%202014.pdf (last visited July 21, 2016).

[6] *Id*. at ¶17.

[7] See, http://krebsonsecurity.com/2016/05/wendys-breach-affected-5-of-restaurants/ (last visited July 21, 2016).

D. Wendy's Failed to Comply With Industry Standards

36. Payment Card Data ("PCD") is heavily regulated. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment. [8]

37. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[9] PCI DSS sets the minimum level of what must be done, not the maximum.

38. PCI DSS 3.1, the version of the standards in effect at the time of the Data Breach, impose the following mandates on Wendy's: [10]

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

39. Among other things, PCI DSS required Wendy's to properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against

[8] *Payment Card Industry Data Security Standard* v3.1, p. 5 (April 2015) available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf (last accessed July 23, 2016).

[9] *Id.*

[10] *Id.*

malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

40. PCI DSS also required Wendy's to not store "the full contents of…the magnetic stripe located on the back of a card" or "the card verification code or value" after authorization.[11]

41. Despite Wendy's awareness of its data security obligations, Wendy's treatment of PCD and PII entrusted to it by its customers fell far short of satisfying Wendy's legal duties and obligations, and included violations of the PCI DSS. Wendy's failed to ensure that access to its data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

E. Wendy's Failed to Upgrade its Payment Systems to Use EMV Technology

42. The payment card industry also sets rules requiring all businesses to upgrade to new card readers that accept EMV chips. EMV chip technology uses embedded computer chips instead of magnetic stripes to store PCD. The magnetic stripe on the back of a debit or credit card contains a code that is recovered by sliding the card through a magnetic stripe reader. The code never changes. Unlike magnetic stripe technology, in which the card information never changes, EMV technology creates a unique transaction code every time the chip is used. Such technology increases payment card security because the unique transaction code cannot be used again, making it more difficult for criminals to use stolen EMV chip card information.

43. The payment card industry, including Visa, MasterCard, and American Express, set a deadline of October 1, 2015 for businesses to transition their POS systems from magnetic stripe readers to readers using EMV chip technology.

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

44. Upon information and belief, Wendy's failed to meet the October 1, 2015 deadline for installing EMV chip readers at its restaurants.

45. Under card operating regulations, businesses that continue accepting payment cards using magnetic stripe readers after the October 1, 2015 deadline are liable for damages resulting from any data breaches.[12]

F. Wendy's Failed to Comply With FTC Requirements

46. In 2011, the Federal Trade Commission ("FTC") updated its 2007 publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[13] 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 to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

47. In July 2015, the FTC supplemented those guidelines with is publication *Start With Security*.[14] In these guidelines, the FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods

---

[12] *See*, http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/ (last visited July 28, 2016).

[13] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (last visited July 23, 2016).

[14] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 23, 2016).

for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

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

G. The Data Breach

50. In the fall of 2015, hackers accessed the computer systems at Wendy's locations throughout the United States, including locations in this District, and installed malicious malware on point-of-sale (POS) systems allowing for the thieves to download and steal copies of Wendy's customers' Customer Data.

51. In early January 2016, because of the rise of fraudulent charges on consumers' credit and debit cards, payment card industry contacts alerted Wendy's of a potential breach.

52. Rather than confirming the Data Breach, on January 27, 2016, Wendy's issued a self-serving statement that it was investigating a potential breach.[15]

53. On February 9, 2016, buried in a press release regarding 2015 sales results, Wendy's confirmed that it had discovered malicious software installed on its POS systems.[16] Wendy's released very few details, but did acknowledge the weakness of its security system at the time of the Data Breach. Further, Wendy's stated that since the Data Breach it had taken

[15] Wendy's Probes Reports of Credit Card Breach, Krebs on Security (Jan. 27, 2016) available at http://krebsonsecurity.com/2016/01/wendys-probes-reports-of-credit-card-breach/ (last accessed July 23, 2016).

[16] See, http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle&ID=2136634 (last accessed July 23, 2016).

steps to strengthen the security of its systems. Despite having confirmatory evidence of the breach, Wendy's still did not publicly disclose to its customers that its payment systems had been breached.

54. On May 11, 2016, Wendy's issued a press release to report on its first-quarter 2016 sales results.[17] Within this sales report, Wendy's stated that it had discovered malicious software designed to steal credit and debit card data on computers that operate the payment processing systems for Wendy's restaurants. The statement said that preliminary findings indicated that the breach resulted from the compromise of a third-party vendor with access to its system. The statement, which was buried in this press release, feebly confirmed the Data Breach, but failed to elucidate the severity of the breach or provide customers with any other relevant information. Indeed, the release was not intended to warn Wendy's customers, the victims of the data breach; it was a financial press release for an audience of investors and securities analysts. Wendy's stated that only "one particular point of sale system" used at "fewer than 300" of its restaurants had been affected. Notably, Wendy's stated emphatically for the second time that it had "disabled and eradicated the malware in affected restaurants."

55. On June 9, 2016, six months after first discovering the Data Breach, Wendy's finally broke its silence and directly addressed the Data Breach in a press release.[18] Wendy's announced that it had found a variation of the malware installed on its POS systems, meaning, without expressing it, that its customers had continued to be at risk for having their Customer Data stolen for six months beyond Wendy's initial oblique mention of the Data Breach. While acknowledging a "series of cybersecurity attacks," Wendy's said only that it "now expected" the number of affected stores to be "considerably higher" than the 300 initially reported.

[17] See, http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle&ID=2167361 (last accessed July 23, 2016).

[18] See, http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle&ID=2176721 (last visited July 23, 2016).

56. The June 9, 2016 press release was simply an attempt to downplay the severity of the incident rather than serve as an explicit warning to customers that their personal and financial data had been stolen.

57. Customers who actually stumbled across Wendy's uninformative and self-serving news release would read a statement from Wendy's that contained numerous material omissions:

a. Wendy's failed to provide a general description of the nature of the Data Breach;

b. Wendy's failed to disclose the number of debit and credit cards compromised;

c. Wendy's failed to disclose how many individuals were affected;

d. Wendy's failed to disclose what customer information was actually compromised; and,

e. Wendy's failed to state that the threat was ongoing.

58. On July 7, 2016, Wendy's issued another press release, this time also emailing the release to customers registered for its "WendyMail" service, announcing that at least 1,025 of its approximately 5,500 franchised restaurants, or 20%, had been affected by the Data Breach.[19] Wendy's, however, did not place any notices in newspapers or in its stores. In the press release, Wendy's provided the address of a webpage that presented a searchable list of affected locations and the likely timeframe each of the affected locations was impacted by the Data Breach.

59. The affected locations website is not very user friendly in terms of information being quickly and easily obtained.[20] The website does not contain an actual listing of potentially affected sites showing all of the locations in one place or that can be search with a basic keyword search; instead, the user must go through a multi-step process to determine if a particular location was affected. The search function requires the user to first select a state and then a city, after

[19] *See*, http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle&ID=2182670 (last visited July 23, 2016).

[20] *See*, https://payment.wendys.com/paymentcardcheck.html (last visited July 29, 2016).

which a list of potentially affected sites is populated for review. This multi-step search returns a narrowed list of restaurants by address. The store number, however, is not listed and that number is used most often to identify charges on bank card statements.

60. In the July 7, 2016 press release, Wendy's offered "one year of complimentary fraud consultation and identity restoration services to all customers who used a payment card at a potentially affected restaurant during the time when the restaurant may have been affected" as long as the customer calls a toll-free number from 8:00 am – 5:30 pm CST, Monday through Friday to receive the information as to how to access these services. Thus, while Wendy's purported to offer its customers a year of free credit monitoring, the majority of Wendy's customers were not made aware of this offer, the limitations on who was eligible for the service, or the hurdles required to sign up for the service.

61. While no specifics have been disclosed, Wendy's indicated in this press release that it still believed the Data Breach occurred as a result of "service providers' remote access credentials being compromised, allowing access – and ability to deploy malware – to some franchisees' point-of-sale systems."

62. Wendy's was not without warning of security threats posed by the use of third party vendors with access to the company's data system. In 2013, the nation's second largest retailer, Target, became of the victim of a well-publicized data breach. Similar to the present case, the Target data breach was the result of hackers using the credentials of a third party vendor to install data-stealing malware into Target's in-store cash registers via remote upload over the Target network. The Target data breach received worldwide attention and put the entire retail industry on notice that lax data security could and would be exploited on a massive scale.

63. Wendy's has failed to provide information as to why it took so long to stop the Data Breach after initially discovering it in January 2016, why it took seven months for it to provide limited information to customers that stumbled across a press release on Wendy's website or that participated in WendyMail, or why it has yet to provide full information to all of its customers. From January 2016 until July 2016, Wendy's stated at least three times that the malware had been eliminated, but now acknowledges that the Data Breach continued at least through June 8, 2016.

64. From January 2016 until July 2016, while Wendy's investigation continued, after the initial complaint in this matter was filed, and while Wendy's motion to dismiss was pending, Wendy's continued to accept its customers' payment cards, exposing their personal and financial data, without any notice to customers that its payment systems were not secure. During this time, Wendy's either knew that its systems were not secure or knew that it could not be certain that its systems were completely secure.

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

66. While many retailers have responded to recent breaches by adopting technology and security practices that help make transactions and stored data more secure, Wendy's has acknowledged that it did not do so.

67. Wendy's failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Customer Data compromised in the Data Breach.

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

68. Without detailed disclosure to Wendy's customers, consumers, including Plaintiffs and Class members, have been left exposed, unknowingly and unwittingly, for at least nine months to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

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

70. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[21] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[22]

71. Thieves are already using the Customer Data stolen from Wendy's to commit actual fraud, as occurred to Plaintiffs as alleged herein.

72. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. The information Wendy's compromised, including Plaintiffs' identifying information and/or other financial information, is "as good as gold" to identity thieves, in the words of the FTC.[23] Identity theft occurs when someone uses another's PII, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

[21] 17 C.F.R § 248.201 (2013).

[22] *Id.*

[23] FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* http://www.vanderbilt.edu/PersonalIdentityTheftProtection.pdf (last visited July 29, 2016).

73. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[24]

74. Identity thieves can use personal information, such as that of Plaintiffs and Class members, which Wendy's failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

75. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[25]

76. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[26]

[24] FTC, Warning Signs of Identity Theft, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 29, 2016).

[25] Victims of Identity Theft, 2014 (Sept. 2015) *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (July 29, 2016).

[26] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited July 29, 2016).

77. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

78. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

I. Plaintiffs and Class Members Suffered Damages

79. The Data Breach was a direct and proximate result of Wendy's failure to properly safeguard and protect Plaintiffs' and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Wendy's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

80. Plaintiffs' and Class members' PII is private and sensitive in nature and was left inadequately protected by Wendy's. Wendy's did not obtain Plaintiffs' and Class members'

[27] GAO, Report to Congressional Requesters, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (last visited July 29, 2016).

consent to disclose their PII to any other person as required by applicable law and industry standards.

81. As a direct and proximate result of Wendy's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

82. Wendy's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

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

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being

placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet card black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their Customer Data;

f. loss of privacy;

g. money paid for food purchased at Wendy's during the period of the Data Breach in that Plaintiffs and Class members would not have dined at Wendy's, or at least would not have used their payment cards for purchases, had Wendy's disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Wendy's provided timely and accurate notice of the Data Breach;

h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

i. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach; loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

83. Acknowledging the repercussions from its wrongful actions and inaction and the resulting Data Breach, Wendy's has made known to customers lucky enough to have stumbled across its press release that it is offering certain customers only one year of credit monitoring and identity theft protection services, despite the fact that it is well known, and acknowledged by the government, that damage and fraud from a data breach can take years to occur. As a result, Plaintiffs and Class members are left to their own actions to protect themselves from the financial damage Wendy's has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Wendy's actions have created for Plaintiffs and Class members, is ascertainable and is a determination appropriate for the trier of fact. Wendy's has also not offered to cover any of the damages sustained by Plaintiffs or Class members.

84. While the Customer Data of Plaintiffs and members of the Class has been stolen, Wendy's continues to hold Customer Data of consumers, including Plaintiffs and Class members. Particularly because Wendy's has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and members of the Class have an undeniable

interest in insuring that their Customer Data is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ACTION ALLEGATIONS

85. Plaintiffs seek relief in their individual capacities and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a Nationwide class defined as follows:

> All persons residing in the United States who made a credit or debit card purchase at Wendy's from October 1, 2015 through the present (the "Nationwide Class").

86. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide class, Plaintiffs assert claims for and on behalf of separate statewide classes for Florida, New York, New Jersey, Texas, and Tennessee, defined as follows:

> All persons residing in [name of State] who made a credit or debit card purchase at Wendy's from October 1, 2015 through the present (the "Statewide Class").

87. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their claims that Wendy's violated state consumer statutes on behalf of separate statewide classes for Florida, New York, New Jersey, Tennessee, and Texas defined as follows:

> All persons residing in [name of State] who made a credit or debit card purchase at Wendy's from October 1, 2015 through the present (the "Statewide Consumer Protection Class").

88. Excluded from each of the above Classes are Wendy's, including any entity in which Wendy's has a controlling interest, is a parent or subsidiary, or which is controlled by Wendy's, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Wendy's. Further excluded are any Wendy's franchise owners, including any entity that has a controlling interest in a Wendy's franchise, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of any

Wendy's franchise. Also excluded are the judges and court personnel in this case and any members of their immediate families.

89. **Numerosity. Fed. R. Civ. P. 23(a)(1).** The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, Wendy's has acknowledged that debit and credit cards were compromised at approximately 1,025 restaurants in the United States for a time period of at least the fall of 2015 through July 7, 2016, and as referenced in Paragraph 3 above, it is estimated that Wendy's serves approximately 50 million customers per month.

90. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** There are questions of law and fact common to the Class that predominate over any questions affecting only individual Class members, and resolution of these common issues will resolve them for the entire Class. These common questions of law and fact include, without limitation:

a. Whether Wendy's had a duty to protect Customer Data;

b. Whether Wendy's was negligent in failing to implement reasonable security procedures and practices;

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

d. Whether Wendy's was negligent by failing to promptly notify class members their personal information had been compromised;

e. Whether Wendy's was reckless in continuing to accept payment cards from customers while its investigation was pending;

f. Whether Wendy's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Customer Data of Plaintiffs and Class members;

g. Whether class members may obtain injunctive relief against Wendy's to require that it safeguard, or destroy rather than retain the Customer Data of Plaintiffs and Class members;

h. What security procedures and data-breach notification procedure Wendy's should be required to implement as part of any injunctive relief ordered by the Court;

i. Whether Wendy's has an implied contractual obligation to use reasonable security measures;

j. Whether Wendy's has complied with any implied contractual obligation to use reasonable security measures;

k. What security measures, if any, must be implemented by Wendy's to comply with its implied contractual obligations; and,

l. The nature of the relief, including equitable relief, to which Plaintiffs and the Class members are entitled.

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

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

93. **Superiority of Class Action. Fed. R. Civ. P. 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

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

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

96. All members of the proposed Classes are readily ascertainable. Wendy's has access to information regarding which of its restaurants were affected by the Data Breach, the time period of the Data Breach, which customers were potentially affected, as well as addresses and other contact information for millions of members of the Classes, which can be used for providing notice to many Class members.

COUNT I
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

97. Plaintiffs restate and reallege Paragraphs 1 through 966 as if fully set forth herein.

98. Wendy's solicited and invited Plaintiffs and Class members to eat at its restaurants and make purchases using their credit or debit cards. Plaintiffs and Class members

accepted Wendy's offers and used their credit or debit cards to make purchases at Wendy's restaurants during the period of the Data Breach.

99. When Plaintiffs and Class members made and paid for purchases of Wendy's services and products in connection with their meals at Wendy's properties, they provided their Customer Data, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards. In so doing, Plaintiffs and Class members entered into implied contracts with Wendy's pursuant to which Wendy's agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised.

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

101. Plaintiffs and Class members would not have provided and entrusted their PII and PCD, including all information contained in the magnetic stripes of their credit and debit cards, to Wendy's to eat at its restaurants and make purchases in the absence of the implied contract between them and Wendy's.

102. Plaintiffs and Class members fully performed their obligations under the implied contracts with Wendy's.

103. Wendy's breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect the PII and PCD of Plaintiffs and Class members

and by failing to provide timely and accurate notice to them that their Customer Data was compromised as a result of the Data Breach.

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

COUNT II
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

105. Plaintiffs restate and reallege Paragraphs 1 through 96 as if fully set forth herein.

106. Upon accepting and storing the Customer Data of Plaintiffs and Class Members in its computer systems, Wendy's undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Wendy's knew that the Customer Data was private and confidential and should be protected as private and confidential.

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

108. Wendy's breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiffs and Class Members and then by failing to provide Plaintiffs and Class Members any detailed information regarding the breach until July 2016. To date, Wendy's has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

109. Wendy's also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Customer Data. Furthering its dilatory practices, Wendy's failed to provide adequate supervision and oversight of the Customer Data with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Customer Data of Plaintiffs and Class Members, misuse the Customer Data and intentionally disclose it to others without consent.

110. Wendy's breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Customer Data of Plaintiffs and Class Members.

111. Through Wendy's acts and omissions described in this Complaint, including Wendy's failure to provide adequate security and its failure to protect Customer Data of Plaintiffs and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, Wendy's unlawfully breached its duty to use reasonable care to adequately protect and secure Customer Data of Plaintiffs and Class members during the time it was within Wendy's possession or control.

112. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Wendy's prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

113. Upon information and belief, Wendy's improperly and inadequately safeguarded Customer Data of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access.

114. Wendy's failure to take proper security measures to protect sensitive Customer Data of Plaintiffs and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Customer Data of Plaintiffs and Class members.

115. Wendy's failed to take proper security measures to protect Customer Data of Plaintiffs and Class members.

116. Wendy's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Customer Data; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Customer Data of Plaintiffs and Class Members; and failing to provide Plaintiffs and Class Members with timely and sufficient notice that their sensitive Customer Data had been compromised.

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

118. As a direct and proximate cause of Wendy's conduct, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Plaintiffs and Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting

agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
Violation of The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA")
Fla. Stat. Ann. § 501.204(1), *et seq*.
(On behalf of Plaintiff Jonathan Torres and the Florida Consumer Protection Class)

119. Plaintiffs restate and reallege Paragraphs 1 through 966 as if fully set forth herein.

120. Plaintiff Jonathan Torres and members of the Florida Consumer Protection Class (collectively the "Florida Consumer Protection Class") are consumers who used their credit or debit cards to purchase food and drink products for personal, family and household purposes from Wendy's locations in Florida.

121. Wendy's engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of food products, goods or services to consumers, including the Florida Consumer Protection Class.

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

123. The purpose of the FDUTPA is "to protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable,

deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202 (2).

124. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of Florida, Wendy's actions were directed at consumers.

125. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of Florida, Wendy's collected and stored highly personal and private information, including Customer Data belonging to the Florida Consumer Protection Class.

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

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

128. As alleged herein this Complaint, Wendy's engaged in conduct, which included, among other things:

a. failing to adequately secure the Customer Data of the Florida Consumer Protection Class;

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

c. failing to disclose, and the misrepresentation of the material fact, that Wendy's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft;

d. failing to disclose in a timely and accurate manner to the Florida Consumer Protection Class the material fact of the nature and extent of the Wendy's data security breach; and,

e. continuing to accept credit and debit card payments and storage of other personal information after Wendy's knew or should have known of the data breach and before it allegedly remedied the breach.

129. By engaging in the conduct delineated above, Wendy's has violated FDUTPA by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the financial transactions, particularly the security thereof, between Wendy's and its customers for the purchase of food products, goods and services;

c. misrepresenting material facts in the furnishing or sale of food products, goods or services to consumers;

d. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

e. engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

g. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

130. As a direct result of Wendy's violation of FDUTPA, the Florida Consumer Protection Class has suffered actual damages that include:

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

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

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

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

e. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

f. costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;

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

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

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

131. As a result of Wendy's violations of FDUTPA, the Florida Consumer Protection Class is entitled to, and seek, injunctive relief pursuant to Fla. Stat. § 501.211, including but not limited to:

a. Ordering that Wendy's engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Wendy's systems on a periodic basis, and ordering Wendy's to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Wendy's engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Wendy's audit, test, and train its security personnel regarding new or modified procedures;

d. Ordering that Wendy's segment customer data by, among other things, creating firewalls and access controls so that if one area of Wendy's is

compromised, hackers cannot gain access to other portions of Wendy's systems;

e. Ordering that Wendy's purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provision of services;

f. Ordering that Wendy's conduct regular database scanning and securing checks;

g. Ordering that Wendy's routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Wendy's to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

132. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wendy's alleged herein, the Florida Consumer Protection Class also seek reasonable attorneys' fees and costs, as well as damages as prescribed by Fla. Stat. § 501.211(2).

COUNT IV
Violation of The New York Business Law, N.Y. Gen. Bus. Law § 349 *et seq.*
(On behalf of Plaintiffs Christine and Donald Jackson
and the New York Consumer Protection Class)

133. Plaintiffs restate and reallege Paragraphs 1 through 966 as if fully set forth herein.

134. Plaintiffs Christine and Donald Jackson and members of the New York Consumer Protection Class (collectively the "New York Consumer Protection Class") are consumers who

used their credit or debit cards to purchase food and drink products for personal, family and household purposes from Wendy's locations in New York.

135. Wendy's engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of food products, goods or services to consumers, including the New York Consumer Protection Class.

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

137. New York General Business Law § 349 ("NYGBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

138. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of New York, Wendy's actions were directed at consumers.

139. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of New York, Wendy's collected and stored highly personal and private information, including Customer Data belonging to the New York Consumer Protection Class.

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

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

142. As alleged herein this Complaint, Wendy's engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, goods or services to consumers in the state of New York, in violation of NYGBL §349, including but not limited to the following:

a. failing to adequately secure the Customer Data of the New York Consumer Protection Class;

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

c. misrepresenting the material fact that Wendy's would maintain adequate data privacy and security practices and procedures to safeguard Customer Data from unauthorized disclosure, release, data breaches, and cyber attack;

d. misrepresenting the material fact that Wendy's did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the Customer Data of the New York Consumer Protection Class;

e. failing to disclose, and the misrepresenting the material fact, that Wendy's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft;

f. failing to disclose in a timely and accurate manner to the New York Consumer Protection Class the material fact of the nature and extent of the Wendy's data security breach; and,

g. continuing to accept credit and debit card payments and storage of other personal information after Wendy's knew or should have known of the data breach and before it allegedly fixed the breach.

143. By engaging in the conduct delineated above, Wendy's has violated NYGBL §349 by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the financial transactions, particularly the security thereof, between Wendy's and its customers for the purchase of food products, goods and services;

c. misrepresenting material facts in the furnishing or sale of food products, goods or services to consumers;

d. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

e. engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

g. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

144. Wendy's systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of the New York Consumer Protection Class.

145. Wendy's willfully engaged in such acts and practices, and knew that they violated NYGBL §349 or showed reckless disregard for whether they violated NYGBL §349.

146. As a direct result of Wendy's violation of NYGBL §349, the New York Consumer Protection Class has suffered actual damages that include:

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

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

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

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

e. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

f. costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;

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

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

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

147. As a result of Wendy's violations of NYGBL §349, the New York Consumer Protection Class is entitled to, and seek, injunctive relief, including but not limited to:

a. Ordering that Wendy's engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Wendy's systems on a periodic basis, and ordering Wendy's to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Wendy's engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Wendy's audit, test, and train its security personnel regarding new or modified procedures;

d. Ordering that Wendy's segment customer data by, among other things, creating firewalls and access controls so that if one area of Wendy's is compromised, hackers cannot gain access to other portions of Wendy's systems;

e. Ordering that Wendy's purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provision of services;

f. Ordering that Wendy's conduct regular database scanning and securing checks;

g. Ordering that Wendy's routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Wendy's to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

148. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wendy's alleged herein, the New York Consumer Protection Class seeks relief under NYGBL §349(h), including, but not limited to, actual or statutory damages, whichever is greater, treble damages, statutory damages, injunctive relief, and attorneys' fees and costs.

COUNT V
Violation of The Tennessee Consumer Protection Act,
Tenn. Code Ann. §§ 47-18-101, *et seq*.
(On behalf of Plaintiff Ashley McConnell and the Tennessee Consumer Protection Class)

149. Plaintiffs restate and reallege Paragraphs 1 through 966 as if fully set forth herein.

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

151. Wendy's engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of food products, goods or services to consumers, including the Tennessee Consumer Protection Class.

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

153. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-101, *et seq*., prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of Tennessee.

154. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of Tennessee, Wendy's actions were directed at consumers.

155. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of Tennessee, Wendy's collected and stored highly personal and private information, including Customer Data belonging to the Tennessee Consumer Protection Class.

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

157. Wendy's should have disclosed this information regarding its computer systems and data security practices because Wendy's was in a superior position to know the true facts

related to the defect, and the Tennessee Consumer Protection Class could not reasonably be expected to learn or discover the true facts.

158. As alleged herein this Complaint, Wendy's engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, goods or services to consumers in the state of Tennessee, in violation of Tenn. Code Ann. § 47-18-104, including but not limited to the following:

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

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

c. misrepresenting the material fact that Wendy's would maintain adequate data privacy and security practices and procedures to safeguard Customer Data from unauthorized disclosure, release, data breaches, and theft in violation of Tenn. Code Ann. § 47-18-104(b)(5) and (9);

d. misrepresenting the material fact that Wendy's did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the Customer Data of the Tennessee Consumer Protection Class in violation of Tenn. Code Ann. § 47-18-104(b)(5) and (9);

e. failing to disclose, and the misrepresenting the material fact, that Wendy's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft in violation of Tenn. Code § 47-18-104(b)(5) and (9);

f. failing to disclose in a timely and accurate manner to the Tennessee Consumer Protection Class the material fact of the nature and extent of the Wendy's data security breach in violation of Tenn. Code Ann. § 47-18-2107(b); and,

g. continuing to accept credit and debit card payments and storage of other personal information after Wendy's knew or should have known of the data breach and before it allegedly remedied the breach.

159. By engaging in the conduct delineated above, Wendy's has violated the Tennessee Consumer Protection Act by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the financial transactions, particularly the security thereof, between Wendy's and its customers for the purchase of food products, goods and services;

c. misrepresenting material facts in the furnishing or sale of food products, goods or services to consumers;

d. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

e. engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

g. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial. Wendy's systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of the Tennessee Consumer Protection Class.

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

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

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

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

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

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

e. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

f. costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;

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

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

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

162. As a result of Wendy's violations of the Tennessee Consumer Protection Act, the Tennessee Consumer Protection Class is entitled to, and seek, injunctive relief, including but not limited to:

a. Ordering that Wendy's engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Wendy's systems on a periodic basis, and ordering Wendy's to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Wendy's engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Wendy's audit, test, and train its security personnel regarding new or modified procedures;

d. Ordering that Wendy's segment customer data by, among other things, creating firewalls and access controls so that if one area of Wendy's is

compromised, hackers cannot gain access to other portions of Wendy's systems;

e. Ordering that Wendy's purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provision of services;

f. Ordering that Wendy's conduct regular database scanning and securing checks;

g. Ordering that Wendy's routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Wendy's to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

163. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wendy's alleged herein, the Tennessee Consumer Protection Class seeks relief under Tenn. Code Ann. § 47-18-109, including, but not limited to, actual damages, treble damages for each willful or knowing violation, injunctive relief, and attorneys' fees and costs.

COUNT VI

Violation of New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*

(On behalf of Plaintiff Gerald Thomas and the New Jersey Consumer Protection Class)

164. Plaintiffs restate and reallege Paragraphs 1 through 966 as if fully set forth herein.

165. Plaintiff Gerald Thomas and members of the New Jersey Consumer Protection Class (collectively the "New Jersey Consumer Protection Class") are consumers who used their

credit or debit cards to purchase food and drink products for personal, family and household purposes from Wendy's locations in New Jersey.

166. Wendy's engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of "merchandise" to consumers, including the New Jersey Consumer Protection Class, as defined by N.J. Stat. Ann. § 56:8-1.

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

168. The New Jersey Consumer Fraud Act ("NJCFA"), N.J. Stat. Ann. § 56:8-2, *et seq*., prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New Jersey.

169. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of New Jersey, Wendy's collected and stored highly personal and private information, including Customer Data belonging to the New Jersey Consumer Protection Class.

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

171. Wendy's should have disclosed this information regarding its computer systems and data security practices because Wendy's was in a superior position to know the true facts

related to the defect, and the New Jersey Consumer Protection Class could not reasonably be expected to learn or discover the true facts.

172. As alleged herein this Complaint, Wendy's engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, goods or services to consumers in the state of New Jersey, in violation of NJCFA, including but not limited to the following:

a. failing to adequately secure the Customer Data of the New Jersey Consumer Protection Class;

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

c. misrepresenting the material fact that Wendy's would maintain adequate data privacy and security practices and procedures to safeguard Customer Data from unauthorized disclosure, release, data breaches, and theft;

d. misrepresenting the material fact that Wendy's did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the Customer Data of the New Jersey Consumer Protection Class;

e. knowingly omitting, suppressing, and concealing the material fact that Wendy's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, with the intent that others rely upon the omission, suppression, and concealment;

f. failing to disclose in a timely and accurate manner to the New Jersey Consumer Protection Class the material fact of the nature and extent of the Wendy's data security breach; and,

g. continuing to accept credit and debit card payments and storage of other personal information after Wendy's knew or should have known of the data breach and before it allegedly remedied the breach.

173. By engaging in the conduct delineated above, Wendy's has violated NJCFA by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the financial transactions, particularly the security thereof, between Wendy's and its customers for the purchase of food products, goods and services;

c. misrepresenting material facts in the furnishing or sale of food products, goods or services to consumers;

d. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

e. engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. engaging in conduct that is immoral, unethical, oppressive and unscrupulous;

g. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

h. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

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

175. As a direct result of Wendy's violation of NJCFA, the New Jersey Consumer Protection Class has suffered ascertainable losses and actual damages that include:

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

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

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

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

e. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

f. costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;

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

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

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

176. As a result of Wendy's violations of NJCFA, the New Jersey Consumer Protection Class is entitled to, and seek, injunctive relief, including but not limited to:

a. Ordering that Wendy's engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Wendy's systems on a periodic basis, and ordering Wendy's to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Wendy's engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Wendy's audit, test, and train its security personnel regarding new or modified procedures;

d. Ordering that Wendy's segment customer data by, among other things, creating firewalls and access controls so that if one area of Wendy's is

compromised, hackers cannot gain access to other portions of Wendy's systems;

e. Ordering that Wendy's purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provision of services;

f. Ordering that Wendy's conduct regular database scanning and securing checks;

g. Ordering that Wendy's routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Wendy's to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

177. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wendy's alleged herein, the New Jersey Consumer Protection Class seeks relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

COUNT VII
Violation of Texas Deceptive Trade Practices – Consumer Protection Act, Tex. Bus. & Com. Code Ann.§ 17.41, *et seq.*
(On behalf of Plaintiff Roxanne Gant and the Texas Consumer Protection Class)

178. Plaintiffs restate and reallege Paragraphs 1 through 966 as if fully set forth herein.

179. Plaintiff Roxanne Gant and members of the Texas Consumer Protection Class (collectively the "Texas Consumer Protection Class") are consumers who used their credit or

debit cards to purchase food and drink products for personal, family and household purposes from Wendy's locations in Texas.

180. Wendy's engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of food products, goods or services to consumers, including the Texas Consumer Protection Class.

181. Wendy's is engaged in, and its acts and omissions affect, trade and commerce. Wendy's relevant acts, practices and omissions complained of in this action were done in in connection with Wendy's business of marketing, offering for sale and selling food products, goods and services to consumers throughout the state of Texas and the United States.

182. The Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), Tex. Bus. & Com. Code Ann. § 17.41, *et seq*., prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of Texas.

183. In the conduct of its business, trade, and commerce, and in the sale of food products, goods or services to consumers in the state of Texas, Wendy's collected and stored highly personal and private information, including Customer Data belonging to the Texas Consumer Protection Class.

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

185. Wendy's should have disclosed this information regarding its computer systems and data security practices because Wendy's was in a superior position to know the true facts

related to the defect, and the Texas Consumer Protection Class could not reasonably be expected to learn or discover the true facts.

186. As alleged herein this Complaint, Wendy's engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, goods or services to consumers in the state of Texas, in violation of DTPA, including but not limited to the following:

a. failing to adequately secure the Customer Data of the Texas Consumer Protection Class;

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

c. misrepresenting the material fact that Wendy's would maintain adequate data privacy and security practices and procedures to safeguard Customer Data from unauthorized disclosure, release, data breaches, and cyber attack;

d. misrepresenting the material fact that Wendy's did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the Customer Data of the Texas Consumer Protection Class;

e. failing to disclose, and the misrepresenting the material fact, that Wendy's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft;

f. failing to disclose in a timely and accurate manner to the Texas Consumer Protection Class the material fact of the nature and extent of the Wendy's data security breach;

g. taking advantage of the lack of knowledge, ability, experience, or capacity of the Texas Consumer Protection Class to a grossly unfair degree; and,

h. continuing to accept credit and debit card payments and storage of other personal information after Wendy's knew or should have known of the data breach and before it allegedly fixed the breach.

187. By engaging in the conduct delineated above, Wendy's has violated DTPA by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the financial transactions, particularly the security thereof, between Wendy's and its customers for the purchase of food products, goods and services;

c. misrepresenting material facts in the furnishing or sale of food products, goods or services to consumers;

d. engaging in conduct that has the capacity or tendency to deceive an average consumer acting reasonably under the circumstances;

e. engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

g. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

188. The Texas Consumer Protection Class relied to their detriment upon Wendy's unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices delineated above.

189. As a direct result of Wendy's violation of DTPA, the Texas Consumer Protection Class has suffered actual damages that include:

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

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

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

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

e. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

f. costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;

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

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

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

190. As a result of Wendy's violations of DTPA, the Texas Consumer Protection Class is entitled to, and seek, injunctive relief, including but not limited to:

a. Ordering that Wendy's engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Wendy's systems on a periodic basis, and ordering Wendy's to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Wendy's engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Wendy's audit, test, and train its security personnel regarding new or modified procedures;

d. Ordering that Wendy's segment customer data by, among other things, creating firewalls and access controls so that if one area of Wendy's is compromised, hackers cannot gain access to other portions of Wendy's systems;

e. Ordering that Wendy's purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provision of services;

f. Ordering that Wendy's conduct regular database scanning and securing checks;

g. Ordering that Wendy's routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Wendy's to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

191. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wendy's alleged herein, the Texas Consumer Protection Class seeks relief under Tex. Bus. & Com. Code Ann. § 17.50, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Wendy's as follows:

a. For an Order certifying the Nationwide Class, or alternatively the Statewide Classes, and the Statewide Consumer Protection Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class, or alternatively the Statewide Classes, and the Statewide Consumer Protection Classes;

b. For equitable relief enjoining Wendy's from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' Customer Data, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

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

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

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

f. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: April 3, 2017

Respectfully submitted,

/s/ John A. Yanchunis
JOHN A. YANCHUNIS
Florida Bar No. 324681
jyanchunis@ForThePeople.com
MARCIO W. VALLADARES
Florida Bar No. 986917
mvalladares@ForThePeople.com
PATRICK A. BARTHLE II
Florida Bar No. 99286
pbarthle@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

JEAN SUTTON MARTIN
Admitted Pro Hac Vice
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road Suite 225
Wilmington, NC 28403
Telephone: (910) 292-6676
Facsimile: (888) 316-3489
jean@jsmlawoffice.com

Ariana J. Tadler
Admitted Pro Hac Vice
Charles Slidders
Admitted Pro Hac Vice
MILBERG LLP
One Pennsylvania Plaza, 50th Floor
New York, New York 10119-0165
Telephone: (212) 946-9453
Facsimile: (212) 868-1229
atadler@milberg.com
cslidders@milberg.com

John G. Emerson*
Emerson Scott, LLP
830 Apollo Lane
Houston, TX 77058
Tel.: (281) 488-8854
Fax: (281) 488-8867
jemerson@emersonfirm.com

David G. Scott*
1301 Scott Street
Little Rock, AR 72202
Tel.: (501) 907-2555
Fax: (501) 907-2556
dscott@emersonfirm.com

Jeremy M. Glapion*
Glapion Law Firm
1704 Maxwell Drive
Wall, NJ 07719
Tel.: (732) 455-9737
jmg@glapionlaw.com

*Pro Hac Application to be submitted

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on April 3, 2017, a true and correct copy of the foregoing Second Amended Complaint was electronically filed with the Clerk of Court using CM/ECF. Copies of the foregoing document will be served upon interested counsel via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ John A. Yanchunis