

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

JAMES GRAHAM, Derivatively on Behalf of
Nominal Defendant, THE WENDY'S COMPANY,

Plaintiffs,

vs.

NELSON PELTZ, PETER W. MAY, EMIL J.
BROLICK, CLIVE CHAJET, EDWARD P.
GARDEN, JANET HILL, JOSEPH A. LEVATO,
J. RANDOLPH LEWIS, PETER H.
ROTHSCHILD, DAVID E. SCHWAB II,
ROLAND C. SMITH, RAYMOND S. TROUBH,
JACK G. WASSERMAN, MICHELLE "MICH"
J. MATHEWS-SPRADLIN, DENNIS M. KASS,
MATTHEW PELTZ, TODD A. PENEGOR and
ROBERT D. WRIGHT,

Defendants,

and

THE WENDY'S COMPANY,

Nominal Defendant.

CASE NO.: 1:16-cv-1153

**VERIFIED SHAREHOLDER
DERIVATIVE COMPLAINT**
(JURY TRIAL DEMANDED)

INTRODUCTION

Plaintiff James Graham ("Plaintiff"), by and through his undersigned attorneys, submits this Verified Shareholder Derivative Complaint (the "Complaint") against defendants named herein. Plaintiff alleges the following based upon information and belief, except as to those allegations concerning Plaintiff, which are alleged upon personal knowledge. Plaintiff's information and belief is based upon, among other things, the investigation conducted by and under the supervision of his counsel which included, among other things: (a) a review and analysis of regulatory filings filed by The Wendy's Company ("Wendy's" or the "Company")

with the United States Securities and Exchange Commission (“SEC”); (b) a review and analysis of press releases and media reports issued and disseminated by Wendy’s; (c) a review of other publicly available information concerning Wendy’s, including articles in the news media and analyst reports; and (d) complaints and related materials in litigation commenced against some or all of the Individual Defendants and/or the Company.

SUMMARY OF THE ACTION

1. This is a shareholder’s derivative action brought for the benefit of Nominal Defendant Wendy’s. Wendy’s is the world’s third largest quick-service restaurant company in the hamburger sandwich segment. Wendy’s is primarily engaged in the business of operating, developing and franchising a system of distinctive quick-service restaurants serving high quality food. It maintains over 6,000 Wendy’s establishments in North America, with a majority franchisee owned and approximately 600 corporate owned. It also has over 400 franchised locations outside North America.

2. This derivative action is brought against certain members of the Company’s Board of Directors (the “Board”) and certain of its executive officers (collectively, the “Individual Defendants”) seeking to remedy the Defendants’ violations of state law and breaches of fiduciary duty during the period beginning October 1, 2012 through the present (the “Relevant Period”).

3. The Individual Defendants’ violations of state law and breaches of fiduciary duty arise out of a data breach that compromised its customers’ personal and financial information that stretched from October 2015 through June 2016 and affected well over 1,000 Wendy’s franchise locations. Wendy’s first reported the Data Breach in January 2016 on the heels of a report issued by noted security blogger Brian Krebs and stated that they had immediately began

an investigation. The Company provided an update on February 9, 2016, informing the public that cybersecurity experts found malware on some of the systems. The Company repeated this same disclosure in its 2015 Form 10-K filed with the SEC on March 3, 2016.

4. Then on May 11, 2016, the Company filed its Form 10-Q for the quarter ended April 3, 2016, and publicly disclosed some additional details about the Data Breach. Wendy's claimed that it believed that malware, installed through the use of compromised third-party credentials, affected one particular point of sale system at fewer than 300 of the approximate 5,500 franchise locations and that the Company's chosen point-of-sale ("POS") system, the Aloha POS system, installed at both corporate owned stores and at a majority of the franchise stores, had not been impacted by the Data Breach. Things got worse.

5. On June 9, 2016, Wendy's issued a press release disclosing that the earlier representations regarding the limited scope of the Data Breach was only the tip of the iceberg. The press release reported that an additional variant of the malware was discovered, and that it had affected a different POS system involving substantially more than the 300 stores already implicated in the Data Breach. As admitted by Wendy's, the Data Breach ran from October 2015 until June 2016, and although discovered in late January 2016, ran unabated for almost an additional six months. Further, in the June 9, 2016 press release, Wendy's did not deny that its chosen POS system for its corporate owned and franchisee stores, the Aloha POS system, had not been implicated in the Data Breach. To this day, the Company has failed to come clean and admit that the Aloha POS system had also been affected by the Data Breach.

6. Further, the Aloha POS system had been mandated for use by Wendy franchisees beginning in October 2012 with a deadline of July 1, 2014 for installation. The Aloha POS system proved fraught with defects from the very beginning and the deadline for installation was

delayed until July 1, 2015, and then again until March 31, 2016, though not all restaurants are required to have the Aloha POS system installed until at least December 31, 2016. It is alleged by one of Wendy's franchisees having over 150 stores that it is unlikely that the December 31, 2016 deadline will be met. And according to this same franchisee, some Wendy's restaurants will never have to install the Aloha POS system.

7. In addition, Plaintiff has not made a demand on Wendy's Board of Directors. Wendy's admits that certain defendants own a substantial amount of Company stock evidencing a controlling interest in the Company. As conceded by the Company, this concentration of ownership gives these defendants "significant influence over the outcome of actions requiring stockholder approval, including the election of directors and the approval of mergers, consolidations and the sale of all or substantially all of the Company's assets." These controlling shareholder defendants also have familial ties with other of the Individual Defendants. Further, other of the Individual Defendants worked at entities other than Wendy's with the controlling shareholder defendants, or were previously management employees at the Company and now are directors beholden to the controlling shareholder defendants. As described in detail in ¶¶ 137-166, for these and other reasons set forth therein, demand would be futile.

8. As a result of the foregoing, the Company is now subjected to a series of class action lawsuits that have been consolidated into two distinct groups: (i) on behalf of financial institutions alleging claims for negligence, negligence per se, violation of the Ohio Deceptive Trade Practices Act, declaratory and injunctive relief (the "Financial Institution Class Action"); and (ii) on behalf of customers of Wendy's alleging claims for breach of implied contract, negligence, violations of state consumer protection laws and violations of state data breach statutes (the "Consumer Class Action"). The cases are currently pending in the United States

District Court for the Western District of Pennsylvania and the United States District Court for the Middle District of Florida, respectively.¹

9. The Individual Defendants breached their duties of loyalty, care and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures with respect to data security for the Company and its franchisees; (ii) failing to exercise their oversight duties by not monitoring the Company and its franchisees' compliance with federal and state laws, payment card industry regulations and its agreements with payment card processors and networks; (iii) failing to cause the Company to make full and fair disclosure concerning (a) the effectiveness of the Company and its franchisees' policies and procedures with respect to data security, and (b) the scope and impact of the Data Breach, resulting in the commencement of the Financial Institutions Class Action and Consumer Class Action; (iv) permitting the Company to violate the Payment Card Industry Data Security Standards ("PCI DSS") by, among other things, (a) allowing Wendy's and many of its franchisees to use the Aloha POS system that the Company knew was fraught with vulnerabilities; (b) failing to ensure that the Company installed and maintained an adequate firewall; (c) failing to ensure that payment card data was properly segmented from the remainder of Wendy's network; (d) failing to implement necessary protocols, such as software image hardening, password protecting programs that captured payment card data and encrypting payment card data at the point-of-sale; and (e) failing to upgrade the Company's systems to utilize EMV technology; (v) consciously disregarding the systemic and pervasive problems with the Aloha POS system; (vi) consciously permitting the Company to maintain an out of date operating system; and

¹ The consolidated cases are docketed at: *First Choice Federal Credit Union et al., v. The Wendy's Company et al.*, Case No.: 2:16-cv-00506 (W.D. PA), and *Jonathan Torres et al. v. Wendy's International LLC*, Case No. 6:16-cv-00210 (M.D. FL).

(vii) failing to exercise their oversight duties commensurate with the risk, given the recognition by senior management and the Board that a security breach could adversely affect the Company's business and operations, as evidenced by the fact that the Data Breach went undetected for several months and, it was not until after receiving questions from a third-party concerning banking industry sources who discovered a pattern of fraud on cards that were used at various Wendy's locations that the Company even publicly acknowledged that it was investigating claims of a possible credit card breach at some locations.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332. There is complete diversity among the parties and the amount in controversy exceeds the sum or value of \$75,000, exclusive of interest and costs.

11. This Court has jurisdiction over each Defendant named herein because each Defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contact with this District so as to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

12. Venue is proper in this Court pursuant to 28 U.S.C. §1391(a) because one or more of the defendants either resides in or maintains executive offices in this District, a substantial portion of the transactions and wrongs complained of herein, including defendants' primary participation in the wrongful acts detailed herein and aiding in violation of fiduciary duties owed to Wendy's occurred in this District and defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that have an effect in this District.

PARTIES

13. Plaintiff James Graham is currently and has continuously been a stockholder of Wendy's since the beginning of the Relevant Period. Plaintiff is a citizen of Oregon.

14. Nominal Defendant Wendy's is incorporated under the laws of the State of Delaware and maintains its headquarters in Dublin, Ohio. Wendy's is the world's third largest quick-service restaurant company in the hamburger sandwich segment. Wendy's is primarily engaged in the business of operating, developing and franchising a system of distinctive quick-service restaurants serving high quality food. As of January 3, 2016, there were 6,076 Wendy's restaurants in operation in North America. Of these restaurants, 632 were operated by Wendy's and 5,444 by a total of 390 franchisees. Also as of January 3, 2016, there were 403 franchised Wendy's restaurants in operation in 27 countries and territories other than North America. Wendy's shares are listed and traded on the NASDAQ Exchange under the Ticker "WEN."

15. Defendant Nelson Peltz ("N. Peltz") has a long standing relationship with Wendy's as both a member of the Company's Board and as a member of management, as well as being a significant beneficial owner of Wendy's stock. He has served as a director of the Company since April 1993 and has served as non-executive Chairman of the Company since June 2007. Prior to that, N. Peltz served as the Company's Chairman and Chief Executive Officer ("CEO") and as a director or manager and an officer of certain of the Company's subsidiaries from April 1993 through June 2007. N. Peltz has been CEO and a founding partner of Trian Fund Management, L.P. ("Trian Partners"), a management company for various investment funds and accounts, since November 2005. From January 1989 to April 1993, N. Peltz was Chairman and CEO of Trian Group, Limited Partnership, which provided investment banking and management services for entities controlled by N. Peltz and Peter W. May. From

1983 to December 1988, N. Peltz was Chairman and CEO and a director of Triangle Industries, Inc. (“Triangle”), a metals and packaging company. Additionally, as of March 28, 2016, N. Peltz was the beneficial owner of 56,520,516 shares (21%) of the Company’s outstanding common stock. Of the over 56 million shares of Wendy’s stock beneficially owned by N. Peltz, 40,792,537 of those shares are owned by Trian Partners and its affiliates. N. Peltz also serves as a director of Mondelez International, Inc. since January 2014, Sysco Corporation since August 2015 and The Madison Square Garden Company since September 2015. He previously served as a director of H. J. Heinz Company from September 2006 to June 2013, Ingersoll Rand plc from August 2012 to June 2014, Legg Mason, Inc. from October 2009 to December 2014 and MSG Networks Inc. from December 2014 to September 2015. According to the Company’s proxy statement filed on Schedule 14A with the SEC on April 11, 2016 (the “2016 Proxy”), the Company touted that N. Peltz “has developed extensive experience working with management teams and boards of directors, as well as in acquiring, investing in and building companies and implementing operational improvements at the companies with which he has been involved. As a result, Mr. Peltz has strong operating experience and strategic planning skills, valuable leadership and corporate governance experience.” Upon information and belief, N. Peltz is a citizen of New York.

16. Defendant Peter W. May (“May”) has a long standing relationship with Wendy’s as both a member of the Company’s Board and as a member of management, as well as being a significant beneficial owner of Wendy’s stock. He has served as a director of the Company since April 1993 and has served as the Company’s non-executive Vice Chairman since June 2007. May served as the President and Chief Operating Officer (“COO”) and as a director or manager and an officer of certain of the Company’s subsidiaries from April 1993 through June 2007.

May has been President and a founding partner of Trian Partners since November 2005. From January 1989 to April 1993, May was President and COO of Trian Group, Limited Partnership. From 1983 to December 1988, he was President and COO and a director of Triangle. As of March 28, 2016, May was the beneficial owner of 56,313,437 (21%) shares of the Company's outstanding common stock. Of the over 56 million shares of Wendy's stock beneficially owned by May, 40,792,537 of those shares are owned by Trian Partners and its affiliates. May has also served as a director of Tiffany & Co. since May 2008. According to the 2016 Proxy, the Company touted that May "has developed extensive experience working with management teams and boards of directors, as well as in acquiring, investing in and building companies and implementing operational improvements at the companies with which he has been involved. As a result, Mr. May has strong operating experience and strategic planning skills, valuable leadership and corporate governance experience." Upon information and belief, May is a citizen of Florida.

17. Defendant Emil J. Brolick ("Brolick") has a long standing relationship with Wendy's as both a member of the Company's Board and as a member of management. He has served as a director of the Company since September 2011. Brolick previously served as President and CEO from September 2011 to January 2016, and as CEO until his retirement from management duties on May 26, 2016. Brolick previously worked at Wendy's International for 12 years from 1988 to 2000, last serving as Senior Vice President of New Product Marketing, Research and Strategic Planning. Brolick was COO of Yum! Brands Inc. and President of two of Yum! Brands' U.S. operating segments, Long John Silver's and A&W All American Food Restaurants, from June 2008 to September 2011. From December 2006 to June 2008, he was President of U.S. Brand Building for Yum! Brands. Prior to that, Brolick served as President and

Chief Concept Officer of Taco Bell Corp., a position he held from July 2000 to November 2006. Upon information and belief, Brolick is a citizen of Ohio.

18. Defendant Janet Hill (“Hill”) is a long time director of the Company. She has served as a director of the Company since September 2008. She previously served as a director of Wendy’s International from 1994 until its merger with the Company in September 2008. Hill also serves as a director of Dean Foods Company since December 2001 and Carlyle Group Management L.L.C., the general partner of the Carlyle Group L.P., since May 2012. Hill previously served as a director of Sprint Nextel Corporation from 2005 to July 2013. She is also a member of the board of directors at two private companies, Echo360, Inc. and Esquire Bank. Upon information and belief, Hill is a citizen of Virginia.

19. Defendant Dennis M. Kass (“Kass”) has served as a director of the Company since December 2015. Kass also serves as an Advisory Partner of Trian Partners, an entity in which defendants N. Peltz, May, and Garden have a controlling interest, and was hired by Trian Partners in January 2015 as a founding member, on the heels of his appointment as a Wendy’s director. As part of his duties at Trian Advisory Partners, Kass may join the Boards of Directors of companies in which Trian Partners invests, such as Wendy’s. Kass also works with defendant M. Peltz, who is a member of the Investment Team of Trian Partners. Upon information and belief, Kass is a citizen of Florida.

20. Defendant Joseph A. Levato (“Levato”) has been either a director and/or member of Wendy’s management since 1993. He has served as a director of the Company since June 1996. Levato served as Executive Vice President (“EVP”) and Chief Financial Officer (“CFO”) of the Company and certain of its subsidiaries from April 1993 to August 1996, when he retired from the Company. Levato worked with defendants N. Peltz and May at Trian Group, Limited

Partnership and Triangle. He was Senior Vice President and Chief Financial Officer of Trian Group, Limited Partnership from January 1992 to April 1993. From 1984 to December 1988, Levato served as Senior Vice President and CFO of Triangle. Upon information and belief, Levato is a citizen of New Jersey.

21. Defendant Michelle “Mich” J. Mathews-Spradlin (“Mathews-Spradlin”) has served as a director of the Company since February 2015. From 1993 until her retirement in 2011, Mathews-Spradlin worked at Microsoft Corporation, where she served as Chief Marketing Officer (“CMO”) and Senior Vice President, Central Marketing Group from 2005 to 2011, Corporate Vice President, Marketing from 2001 to 2005, Vice President, Corporate Public Relations from 1999 to 2001 and head of the Corporate Public Relations function from 1993 to 1999. Prior to her employment at Microsoft, Mathews-Spradlin worked in the United Kingdom as a communications consultant for Microsoft from 1989 to 1993. Prior to that, she held various positions at General Motors Co. from 1986 to 1989. Mathews-Spradlin also serves as a Board member at several private companies, including Bitium, Inc., OANDA Global Corporation, The Bouqs Company and You & Mr. Jones. According to the 2016 Proxy, the Company touts that Mathews-Spradlin “possesses extensive experience in global brand management and a deep understanding of the technology industry attributable to her background as a senior executive at Microsoft Corporation.” Upon information and belief, Mathews-Spradlin is a citizen of California.

22. Defendant Matthew H. Peltz (“M. Peltz”) has served as a director of Wendy’s since December 2015 and is the son of defendant N. Peltz. M. Peltz also works with defendants N. Peltz, May, Kass, and Garden at Trian Partners. He is a Partner and has been a member of the Investment Team of Trian Partners since January 2008. Prior to that, he was with Goldman

Sachs & Co. from May 2006 to January 2008, where he worked as an investment banking analyst and subsequently joined Liberty Harbor, an affiliated multi-strategy hedge fund. M. Peltz previously served as a director of ARG Holding Corporation, the parent company of the Arby's restaurant brand, from September 2012 to December 2015. Upon information and belief, M. Peltz is a citizen of New York.

23. Defendant Todd A. Penegor ("Penegor") has served as a director of the Company since May 2016 and as CEO of the Company since May 27, 2016. Penegor joined the Company in June 2013 and served as the President and CFO of Wendy's from January 2016 to May 2016. Penegor previously served as Executive Vice President, CFO and International from December 2014 to January 2016 and as Senior Vice President and CFO from September 2013 to December 2014. Prior to joining the Company, Penegor worked at Kellogg Company, a global leader in food products, from 2000 to 2013 where he held several key leadership positions, including Vice President of Kellogg Company and President of U.S. Snacks from 2009 to June 2013, Vice President and CFO of Kellogg Europe from 2007 to 2009 and Vice President and CFO of Kellogg USA and Kellogg Snacks from 2002 to 2007. Prior to joining Kellogg, Penegor worked for 12 years at Ford Motor Company in various positions. According to the Company's proxy statement filed on Schedule 14A with the SEC on April 17, 2015 (the "2015 Proxy"), the Company stated that Penegor, "who was promoted from Senior Vice President and Chief Financial Officer to Executive Vice President, Chief Financial Officer and International, took on additional oversight of the Company's International division, in addition to maintaining his existing responsibilities for Finance, Development and Information Technology." Upon information and belief, Penegor is a citizen of South Carolina.

24. Defendant Peter H. Rothschild (“Rothschild”) has served as a director of Wendy’s and its subsidiaries for over a decade. He has been a director of the Company since May 2010 and served as a director of Wendy’s International from March 2006 until its merger with the Company in September 2008. Rothschild previously served as a director of Deerfield Capital Corp., predecessor to CIFC Corp., from December 2004 to April 2011 and as Interim Chairman of Deerfield Capital’s Board of directors from April 2007 to April 2011. Upon information and belief, Rothschild is a citizen of New York.

25. Defendant Clive Chajet (“Chajet”) was a director of the Company for almost a decade. He served as a director of the Company from June 1994 until his retirement from the Board on May 2014. Upon information and belief, Chajet is a citizen of New York.

26. Defendant Edward P. Garden (“Garden”) has a long standing relationship with Wendy’s as a director and member of management. He served as a director of the Company from December 2004 until his resignation from the Board on December 14, 2015. Garden previously served as Vice Chairman of the Company from December 2004 through June 2007 and as Executive Vice President of the Company from August 2003 until December 2004. Garden works with defendants N. Peltz, May, Kass, and M. Peltz at Trian Partners and is the son-in-law of N. Peltz. He has been Chief Investment Officer and a founding partner of Trian Partners since November 2005. Garden previously served as a director of Trian Acquisition I Corp. from October 2007 to May 2013. He also has served as a director of Family Dollar Stores, Inc. since 2011 and previously served as a director of Chemtura Corporation from January 2007 through March 2009. As of March 28, 2016, Garden was the beneficial owner of 41,032,902 (15.3%) shares of the Company’s outstanding common stock. Of the over 41 million of Wendy’s

stock beneficially owned by Garden, 40, 792,537 of those shares are owned by through Trian Partners and its affiliates. Upon information and belief, Garden is a citizen of Connecticut.

27. Defendant J. Randolph Lewis (“Lewis”) was a director at Wendy’s or its subsidiaries for well over a decade. He served as a director of the Company from September 2008 until his retirement from the Board in May 2016. Lewis previously served as a director of Wendy’s International from 2004 until its merger with the Company in September 2008. Lewis also served as Senior Vice President, Supply Chain and Logistics of Walgreen Co. until his retirement in January 2013. He joined Walgreen Co. in March 1992 as Divisional Vice President, Logistics and Planning and was promoted to Senior Vice President, Supply Chain and Logistics in 1996. Upon information and belief, Lewis is a citizen of Illinois.

28. Defendant David E. Schwab II (“Schwab”) was a director of Wendy’s for over 20 years. He served as a director of the Company from October 1994 until his retirement from the Board in May 2016. Upon information and belief, Schwab is a citizen of New York.

29. Defendant Roland C. Smith (“Smith”) served as a director of the Company from June 2007 until his resignation from the Board in May 2014. Smith previously served as the CEO of the Company from June 2007 to September 2011, as President of the Company from September 2008 to September 2011, and as Special Adviser to the Company from September 2011 to December 2011. Smith also served as CEO of Wendy’s International from September 2008 to September 2011. Smith served as CEO of Arby’s Restaurant Group, Inc. (“Arby’s”) from April 2006 to September 2008, as President of Arby’s from April 2006 to June 2006, and as interim President of Arby’s from January 2010 to May 2010. He currently serves as President and CEO of Delhaize America and as Executive Vice President of Delhaize Group, an international food retailer, positions he has held since October 2012. Previously, Mr. Smith

served as President and CEO of American Golf Corporation and National Golf Properties from February 2003 to November 2005, as President and CEO of AMF Bowling Worldwide, Inc. from April 1999 to January 2003, and as President and as Chief Executive Officer of Arby's, Inc., predecessor to Arby's, from February 1997 to April 1999. He also serves as Chairman of the Board of directors of Carmike Cinemas, Inc. Upon information and belief, Smith is a citizen of Georgia.

30. Defendant Raymond S. Troubh ("Troubh") was a director of Wendy's for almost 20 years. He served as a director of the Company from June 1994 until his retirement from the Board in May 2014. Troubh also serves as a director of Diamond Offshore Drilling, Inc., General American Investors Company and Gentiva Health Services, Inc. Over the course of his career, Troubh has served as a director of over 30 public companies of varying degrees of size and complexity, and has served as chairman of the compensation and audit committee of many of those companies. Upon information and belief, Troubh is a citizen of New York.

31. Defendant Jack G. Wasserman ("Wasserman") was a director at Wendy's for over a decade. He served as a director of the Company from March 2004 until his retirement from the Board in May 2015. Wasserman also serves as a director of Icahn Enterprises G.P., Inc., the general partner of Icahn Enterprises L.P., and previously served as a director of its operating subsidiaries – America Casino & Entertainment Properties LLC, from 2003 until its sale in 2008, and National Energy Group, Inc., from 1998 until its sale in 2006. Upon information and belief, Wasserman is a citizen of New York.

32. Defendant Robert D. Wright ("Wright") has served as Executive Vice President, Chief Operations Officer and International since May 30, 2016. Wright previously served as Executive Vice President, Chief Operations Officer of the Company from December 17, 2014 to

May 30, 2016. Prior to that, Wright served as Chief Operations Officer of the Company from March 10, 2014 to December 17, 2014. According to the 2015 Proxy, the Company stated that “Mr. Wright was promoted to Executive Vice President and Chief Operations Officer and assumed a larger portfolio of customer-facing responsibilities, including in-restaurant technology, restaurant facilities and the continuous improvement of the customer service experience, in addition to maintaining his existing responsibilities for Company and franchise restaurant operations.” According to information and belief, Wright is a citizen of Ohio.

33. Defendants Peltz, May, Brolick, Chajet, Garden, Hill, Levato, Lewis, Rothschild, Schwab, Smith, Wasserman, Mathews-Spradlin, Kass, M. Peltz, Penegor, Troubh and Wright are sometimes collectively referred to herein as the “Individual Defendants.”

34. Defendants Peltz, May, Brolick, Hill, Kass, Levato, Mathews-Spradlin, M. Peltz, Penegor and Rothschild are sometimes collectively referred to herein as the “Current Director Defendants.”

FIDUCIARY DUTIES OF THE INDIVIDUAL DEFENDANTS

35. By reason of their positions as officers, directors and/or fiduciaries of Wendy’s during the Relevant Period and because of their ability to control the business and corporate affairs of the Company, the Individual Defendants owed Wendy’s and its shareholders fiduciary obligations of good faith, loyalty and candor, and were and are required to use their utmost ability to control and manage the Company in a fair, just, honest and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Wendy’s and its shareholders so as to benefit all shareholders equally and not in furtherance of their personal interest or benefit.

36. Each director and officer of the Company owes to Wendy's and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the Company's affairs and in the use and preservation of its property and assets, and the highest obligations of fair dealing.

37. The Individual Defendants, because of their positions of control and authority as directors and/or officers of Wendy's, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the various public statements issued by the Company. Due to their positions with Wendy's, each of the Individual Defendants had knowledge of material non-public information regarding the Company.

38. To discharge their duties, the Individual Defendants were required to exercise reasonable and prudent supervision over the management, policies, practices and controls of the Company. By virtue of such duties, the officers and directors of Wendy's were required to, among other things:

- a. Exercise good faith to ensure that the affairs of the Company were conducted in an efficient, business-like manner so as to make it possible to provide the highest quality performance of their business;
- b. Exercise good faith to ensure that the Company was operated in a diligent, honest and prudent manner and complied with all applicable federal, state and foreign laws, rules, regulations and requirements, and all contractual obligations, including acting only within the scope of its legal authority;
- c. Exercise good faith in supervising the preparation, filing and/or dissemination of financial statements, press releases, audits, reports or other information required

- by law, and in examining and evaluating any reports or examinations, audits, or other financial information concerning the financial condition of the Company;
- d. Refrain from unduly benefiting themselves and other Company insiders at the expense of the Company; and
 - e. When put on notice of problems with the Company's business practices and operations, exercise good faith in taking appropriate action to correct the misconduct and prevent its recurrence.

39. Moreover, Wendy's maintains a Code of Conduct and Ethics (the "Code"), which the Company describes is a "guide to legal and ethical behavior," and applies to directors and employees of the Company. With respect to the responsibility of the Board, the Code states the following, in relevant part:

Wendy's expects the members of its Board of Directors at all times to set the right tone by being mindful of their obligations as fiduciaries and by adhering to high standards of conduct, including the policies set out in this Code. Directors should seek to promote those standards in fulfilling their responsibilities to the Company and its stockholders. Directors must adhere to and promote our "open door" policy described above.

Like our employees, ***directors are expected to act honestly, in compliance with law and in the best interests of the Company and its stockholders.*** They must conduct themselves in a professional manner and act in good faith and with due care. ***In their oversight of management, directors should be vigorous in their inquiries and exercise independent judgment to promote the interests of the Company. Directors are also expected to maintain the confidentiality of Company information*** and to disclose any possible conflicts of interest that they may have with respect to matters being considered by the Board of Directors or any other aspect of the Company's business.

Any director who has concerns about compliance with this Code should direct his or her inquiry to the Chairman of the Audit Committee of the Board of Directors or to the General Counsel of Wendy's.

(Emphasis added).

34. With respect to legal compliance, the Code states the following, in relevant part:

COMPLIANCE WITH LAW

Wendy's strives to be an honorable company and employer. Employees must always operate within the law in all business dealings. *It is the Company's express policy that it and its employees obey all applicable U.S. federal, state and local and international laws and regulations.* Employees have a personal responsibility to become familiar and comply with the laws and regulations related to their job responsibilities. There are also other laws – not directly related to an employee's job but of general relevance to work situations – of which employees should be aware. If employees have any questions about what is within the law and what is not, they should seek advice from the Legal Department. Noted below are some of the most important laws that apply to Wendy's and its employees and business dealings.

(Emphasis added).

35. With respect to business conduct, the Code states the following, in relevant part:

BUSINESS CONDUCT AND CONTACTS

Present the Company Truthfully. Communications should reinforce a sense of trust in the Company. Whether statements are channeled through franchisees, customers, stockholders, the analyst community, suppliers, trade groups, the mass media or made in private conversation, “honesty is the best policy.” *Public statements should be sufficiently candid, clear and complete so that they neither mislead nor lend themselves to misinterpretation.* However, material non-public information may not be disclosed without approval from the Legal Department. *Wendy's is also committed to full compliance with all requirements applicable to its public disclosures and those of Wendy's, including reports filed or furnished to securities regulators by Wendy's. All of our business communications should be timely, clear and accurate.* It is a violation of our policy to misrepresent our financial performance or otherwise compromise the integrity of our financial statements or other disclosures.

All press releases intended for the investor or franchisee communities must first be reviewed and approved by the Legal Department.

(Emphasis added).

36. With respect to Company assets, the Code states the following, in relevant part:

USE OF COMPANY ASSETS

Using Company Computers and Other Technology. Computers and electronic information are essential tools to support our business. . . .

To keep our computer systems and information secure, we need to take necessary actions to safeguard all passwords and identification codes to prevent unauthorized access.

37. With respect to confidential information, the Code states the following, in relevant part:

CONFIDENTIAL AND PROPRIETARY INFORMATION

Company Information. Confidential information includes information regarding the Company's employees, customers . . .

Examples of personal data include personal, employment, medical, financial and education and training information. Most countries have laws regulating the collection and use of personal data, although the types of data covered, the nature of the protection, and local enforcement mechanisms vary. Wendy's policy is to comply with all such applicable laws. All employees are responsible for ensuring compliance with the data privacy requirements under such laws and regulations and under the Company guidelines and policies. Employees may be required to attend training.

38. With respect to personal information, the Code states the following, in relevant part:

Franchisee, Supplier or Customer Information. The nature of Wendy's business gives many employees access to critical business information about franchisees, suppliers and, in some cases, personal information about customers. Maintaining their trust requires that you protect the confidentiality of this information. Information about a franchisee's or supplier's business is confidential as is personal information about customers. Disclosure within the Company should only be on a business "need to know" basis. Disclosure to outsiders, except to comply with legal requirements, is not only inconsistent with this Code but in some cases may also be illegal.

39. Additionally, the Company maintains a set of Corporate Governance Guidelines (amended November 5, 2012) which states the following, in relevant part:

A. Role of Board and Management:

The Company’s Board of Directors (the “Board”), which is elected by the stockholders, is the ultimate decision-making body of the Company, except with respect to matters reserved to the stockholders. The Board selects the Chief Executive Officer and other senior executives of the Company, who are charged with directing the Company’s business. The primary function of the Board, therefore, is oversight—defining and enforcing standards of accountability that enable executive management to execute their responsibilities fully and in the best interests of the Company and its stockholders.

C. Conduct:

Risk Oversight. The Board provides oversight with respect to the Company’s risk assessment and risk management activities, which are designed to identify, prioritize, assess, monitor and mitigate material risks to the Company, including financial, operational, compliance and strategic risks. The Board may from time to time delegate certain aspects of its risk oversight function to one or more of its committees or to members of management as it deems appropriate, each of which shall report directly to the Board.

40. The Company also has an Audit Committee, a Nominating and Corporate Governance Committee, a Compensation Committee and a Performance Compensation Subcommittee, all of which have their own charters setting forth requirements for director qualifications, director responsibilities and director authority.

41. Finally, the Wendy’s Board was responsible for risk oversight:

Board’s Role in Risk Oversight

The Board of Directors provides oversight with respect to the Company’s risk assessment and risk management activities, which are designed to identify, prioritize, assess, monitor and mitigate material risks to the Company, including financial, operational, compliance and strategic risks. While *the Board has primary responsibility for risk oversight*, the Board’s standing committees support the Board by regularly addressing various risks in their respective areas of responsibility. The Audit Committee focuses on financial risks, including reviewing with management, the Company’s internal auditors and the Company’s independent registered public accounting firm the Company’s major risk exposures (with particular emphasis on financial risk exposures), the adequacy

and effectiveness of the Company's accounting and financial controls and the steps management has taken to monitor and control such exposures, including the Company's risk assessment and risk management policies. The Compensation Committee considers risks presented by the Company's compensation policies and practices for its executive officers and other employees, as discussed below under the caption "Compensation Risk Assessment." The Nominating and Corporate Governance Committee reviews risks related to the Company's corporate governance structure and processes, including director qualifications and independence, stockholder proposals related to governance, succession planning and the effectiveness of our Corporate Governance Guidelines. ***The Board's risk oversight function is also supported by a Risk Oversight Committee composed of members of senior management. The Risk Oversight Committee is exclusively devoted to prioritizing and assessing all categories of enterprise risk, including risks delegated by the Board of Directors to the Board committees, as well as other operational, compliance and strategic risks facing the Company.*** Each of these committees reports directly to the Board.

The Board believes that its current leadership structure supports the risk oversight function of the Board. Having the roles of Chief Executive Officer and Chairman of the Board filled by separate individuals allows the Chief Executive Officer to lead senior management in its supervision of the Company's day-to-day business operations, including the identification, assessment and mitigation of material risks, ***and allows the Chairman to lead the Board in its oversight of the Company's risk assessment and risk management activities.***

(Emphasis added).

42. Each Individual Defendant, by virtue of his or her position as a director and/or officer owed to the Company and to its shareholders the fiduciary duty of loyalty, good faith and the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and/or officers of Wendy's, the absence of good faith on their part and a reckless disregard for their duties to the Company and its shareholders that the Individual Defendants were aware or should have been aware posed a risk of serious injury to the Company.

43. The Individual Defendants breached their duties of loyalty, care and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures with respect to data security for the Company and its franchisees; (ii) failing to exercise their oversight duties by not monitoring the Company and its franchisees' compliance with federal and state laws, payment card industry regulations and its agreements with payment card processors and networks; (iii) failing to cause the Company to make full and fair disclosure concerning (a) the effectiveness of the Company and its franchisees' policies and procedures with respect to data security, and (b) the scope and impact of the Data Breach, resulting in the commencement of the Financial Institutions Class Action and Consumer Class Action; (iv) permitting the Company to violate the PCI DSS by, among other things, (a) allowing Wendy's and many of its franchisees to use the Aloha POS system that the Company knew was fraught with vulnerabilities; (b) failing to ensure that the Company installed and maintained an adequate firewall; (c) failing to ensure that payment card data was properly segmented from the remainder of Wendy's network; (d) failing to implement necessary protocols, such as software image hardening, password protecting programs that captured payment card data and encrypting payment card data at the point-of-sale; and (e) failing to upgrade the Company's systems to utilize EMV technology; (v) consciously disregarding the systemic and pervasive problems with the Aloha POS system; (vi) consciously permitting the Company to maintain an out of date operating system; and (vii) failing to exercise their oversight duties commensurate with the risk, given the recognition by senior management and the Board that a security breach could adversely affect the Company's business and operations, as evidenced by the fact that the Data Breach went undetected for several months and, it was not until after receiving questions from a third-party concerning banking industry sources who discovered a pattern of fraud on cards that were

used at various Wendy's locations that the Company even publicly acknowledged that it was investigating claims of a possible credit card breach at some locations.

SUBSTANTIVE ALLEGATIONS

Background

44. Wendy's engages in the business of operating, developing, and franchising a system of quick-service restaurants. It is the parent company of its 100% owned subsidiary holding company Wendy's Restaurants, LLC ("Wendy's Restaurants"). Wendy's Restaurants is the parent company of Wendy's International, LLC, formerly known as Wendy's International, Inc. Wendy's International, LLC is the indirect parent company of Quality Is Our Recipe, LLC ("Quality"), which is the owner and franchisor of the Wendy's[®] restaurant system in the United States.

45. Wendy's corporate predecessor was incorporated in Ohio in 1929 and was reincorporated in Delaware in June 1994. Effective September 29, 2008, in conjunction with the merger with Wendy's, the Company's corporate name was changed from Triarc Companies, Inc. ("Triarc") to Wendy's/Arby's Group, Inc. Effective July 5, 2011, in connection with the sale of Arby's Restaurant Group, Inc. ("Arby's"), Wendy's/Arby's Group, Inc. changed its name to The Wendy's Company.

46. As a franchisor, Wendy's has total control over the manner in which its franchisees operate in order to maintain uniformity from restaurant to restaurant. Wendy's standard Uniform Franchise Agreement emphasizes the importance of "uniform standards, specifications, and procedures for operations[.]" any aspect of "which may be changed, improved, and further developed by [Wendy's] from time to time[.]" The Unit Franchise

Agreement indicates that Wendy's control over franchisee operations extends to "computer software and electronic data transmission systems for point of sale reporting."

47. Similarly, the Company's 2015 Form 10-K also stated that:

Franchised restaurants are required to be operated under uniform operating standards and specifications relating to the selection, quality and preparation of menu items, signage, décor, equipment, uniforms, suppliers, maintenance and cleanliness of premises and customer service. Wendy's monitors franchisee operations and inspects restaurants periodically to ensure that required practices and procedures are being followed.

Background on POS attacks

48. A large portion of Wendy's sales are made to customers who use debit or credit cards. In processing payment card transactions, merchants acquire a substantial amount of information about each customer, including his or her full name; credit or debit card account number; card security code (the value printed on the card or contained in the microprocessor chip or magnetic stripe of a card and used to validate card information during the authorization process); the card's expiration date and verification value; and the PIN number for debit cards. This information typically is stored on the merchants' computer systems and transmitted to third parties to complete the transaction. At other times and for other reasons, merchants also may collect other personally identifiable information about their customers, including but not limited to, financial data, mailing addresses, phone numbers, driver's license numbers, and email addresses.

49. The Individual Defendants were – and at all relevant times have been – aware that the information Wendy's maintains about its customers is highly sensitive and could be used for nefarious purposes by third parties, such as perpetuating identity theft and making fraudulent purchases.

50. The Individual Defendants are – and at all relevant times have been – aware of the importance of safeguarding the Company’s customers’ information and of the foreseeable consequences that would occur if its security systems were breached, specifically including the risk of massive liability to financial institutions and consumers, as well as potential exposure to criminal liability and loss of reputation.

51. Indeed, as early as 2008, Wendy’s identified the potential repercussions of a data security breach as a substantial “Risk Factor” for its business in its annual report and SEC filings, stating: “We rely on computer systems and information technology to run our business. Any material failure, interruption or security breach of our computer systems or information technology may adversely affect the operation of our business and results of operations. We are significantly dependent upon our computer systems and information technology to properly conduct our business. A failure or interruption of computer systems or information technology could result in the loss of data, business interruptions or delays in business operations. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. Any security breach of our computer systems or information technology may result in adverse publicity, loss of sales and profits, penalties or loss resulting from misappropriation of information.”

52. In addition to their general duties to ensure that systems are in place to safeguard customers’ information to prevent the risk of loss, the Individual Defendants were – and at all relevant times have been – obligated to oversee the Company’s compliance with rules governing

payment card transactions, industry standards and various federal and state laws, as well as with the Company's own commitments, internal policies and procedures.

53. Wendy's has continuously acknowledged this legal duty and reassured the public its duty was being met in the Company's "Privacy Policy" posted on its website. For example, the version of the policy in effect on April 29, 2013, told the public that Wendy's "make[s] what [it] believe[s] to be commercially reasonable efforts to provide a reasonable level of security for personal information [the Company is] required to protect."

54. As described below, the Individual Defendants knowingly failed to conduct adequate oversight to ensure that its data security was PCI DSS compliant as required by Wendy's contracts with financial institutions, or meet commercially reasonable efforts for data security as required Wendy's commitment to its customers, as embodied by its Privacy Policy, and once it learned that the Data Breach had occurred knowingly failed to provide timely disclosure to its customers.

The Individual Defendants Knew that a Security Breach Presented a Significant Threat to Wendy's and They Knew that Wendy's Computer Systems Were Vulnerable to Hackers

55. Theft of customer data through breaches of retailers' point of sale systems hit the mainstream in 2007, when TJX Companies Inc. ("TJX") admitted in an SEC filing that at least 45.6 million credit and debit card numbers were stolen from its customers over an 18-month period. In addition, TJX disclosed that personal data provided in connection with the return of merchandise without receipts by about 450,000 customers had been stolen. The breach cost the company over \$250 million, including costs related to improving the company's computer system, as well as costs related to lawsuits, investigations and other claims stemming from the breach.

56. Since that time, reports of breaches of major retailers' point of sale systems became commonplace. In 2013, security blogger Brian Krebs of *KrebsonSecurity* broke the news that Target Corporation ("Target"), the nation's second largest retailer, had been the victim of a massive data breach that exposed personal and financial information of more than 110 million customers. According to Krebs, the attackers hacked into Target's systems by using network credentials of a third-party vendor and installed malicious software that infected point-of-sale systems at Target checkout counters. The malware captured the data stored on a payment card's magnetic stripe in the instant after it has been swiped at the terminal and is still in the system's memory, which the thieves can then use to create cloned copies of the payment cards.

57. During the time of the events complained of herein, the Individual Defendants were well-aware that a data security breach such as the Data Breach that occurred from October 2015 to June 2016 was a substantial "Risk Factor" for the Company.

58. Indeed, as early as 2009, Wendy's identified the potential repercussions of a data security breach as a substantial "Risk Factor" for its business in its annual report filed with the SEC on March 13, 2009 (the "2008 10-K"), stating the following, in relevant part:

We rely on computer systems and information technology to run our business. Any material failure, interruption or security breach of our computer systems or information technology may adversely affect the operation of our business and results of operations.

We are significantly dependent upon our computer systems and information technology to properly conduct our business. A failure or interruption of computer systems or information technology could result in the loss of data, business interruptions or delays in business operations. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. Any security breach of our computer systems or information technology may result in adverse publicity, loss of sales and profits, penalties or loss resulting from misappropriation of information.

59. The foregoing risk factor was repeated in Wendy's Form 10-Ks for Fiscal Years 2009, 2010, 2011, 2012, 2013 and 2014 filed with the SEC on March 4, 2010, March 3, 2011, March 1, 2012, February 28, 2013, February 27, 2014 and February 26, 2015, respectively. Additionally, in the Company's Form 10-K for Fiscal Year 2011, the Company included the following risk factor with respect to safeguarding confidential information of employees and customers:

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.

60. The foregoing risk factor was included in the Company's Form 10-Ks for Fiscal Years 2012, 2013 and 2014.

61. In the Company's 2015 Form 10-K filed with the SEC on March 3, 2016, the Company amended its warnings pertaining to data security to the following, in relevant part:

We are heavily dependent on computer systems and information technology and any material failure, interruption or security breach of our computer systems or technology could impair our ability to efficiently operate our business.

We are significantly dependent upon our computer systems and information technology to properly conduct our business, including point-of-sale processing in our restaurants, management of our supply chain, collection of cash, payment of obligations and various other processes and procedures. Our ability to efficiently manage our business depends significantly on the reliability and capacity of these systems and information technology. The failure of these systems and information technology to operate effectively, an interruption, problems with maintenance, upgrading or transitioning to replacement systems, fraudulent manipulation of sales reporting from our franchised restaurants resulting in loss of

sales and royalty payments, or a breach in security of these systems could be harmful and cause delays in customer service, result in the loss of data and reduce efficiency or cause delays in operations. Significant capital investments might be required to remediate any problems. Any security breach involving our or our franchisees' point-of-sale or other systems could result in a loss of consumer confidence and potential costs associated with fraud. 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 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.

As part of our marketing efforts, we rely on search engine marketing and social media platforms to attract and retain customers. These efforts may not be successful, and pose a variety of other risks, including the improper disclosure of proprietary information, negative comments about the Wendy's brand, exposure of personally identifiable information, fraud or out of date information. The inappropriate use of social media vehicles by franchisees, customers, or employees could increase our costs, lead to litigation or result in negative publicity that could damage our reputation. The occurrence of any such developments could have an adverse effect on business results.

The occurrence of cyber incidents, or a deficiency in cybersecurity, could negatively impact our business by causing a disruption to our operations, a compromise or corruption of confidential information, and/or damage to our employee and business relationships, all of which could subject us to loss and harm the Wendy's brand.

A cyber incident is considered to be any adverse event that threatens the confidentiality, integrity or availability of information resources. More specifically, a cyber incident is an intentional attack or an unintentional event that can include gaining unauthorized access to systems to disrupt operations, corrupt data or steal confidential information about customers, franchisees, vendors and employees. A number of retailers and other companies have recently experienced serious cyber incidents and breaches of their information technology systems. The Company is also investigating unusual credit card activity at some Wendy's restaurants, as further described below. As the Company's reliance on technology has increased, so have the risks posed to its systems, both internal and those it has outsourced. The three primary risks that could directly result from the occurrence of a cyber incident include operational interruption, damage to the relationship with customers, franchisees and employees and private data exposure. In addition

to maintaining insurance coverage to address cyber incidents, the Company has also implemented processes, procedures and controls to help mitigate these risks. However, these measures, as well as its increased awareness of a risk of a cyber incident, do not guarantee that the Company's reputation and financial results will not be adversely affected by such an incident.

Because the Company and its franchisees accept electronic forms of payment from their customers, the Company's business requires the collection and retention of customer data, including credit and debit card numbers and other personally identifiable information in various information systems that the Company and its franchisees maintain and in those maintained by third parties with whom the Company and its franchisees contract to provide credit card processing. The Company also maintains important internal Company data, such as personally identifiable information about its employees and franchisees and information relating to its operations. The Company's use of personally identifiable information is regulated by foreign, federal and state laws, as well as by certain third-party agreements. As privacy and information security laws and regulations change, the Company may incur additional costs to ensure that it remains in compliance with those laws and regulations. If the Company's security and information systems are compromised or if its employees or franchisees fail to comply with these laws, regulations, or contract terms, and this information is obtained by unauthorized persons or used inappropriately, it could adversely affect the Company's reputation and could disrupt its operations and result in costly litigation, judgments, or penalties resulting from violation of federal and state laws and payment card industry regulations. A cyber incident could 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 the Company's business and results of operations.

As reported in the news media in late January, the Company has engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity at some Wendy's restaurants. Out of the locations investigated to date, some have been found by the cybersecurity experts to have malware on a certain system. The investigation is ongoing and the Company is continuing to work closely with cybersecurity experts and law enforcement officials.

62. Further, as set forth in the Company's annual and quarterly financial statements dating back to 2007, the Individual Defendants were aware that they were required to comply with payment card industry rules and that a failure to do so may adversely affect the Company's ability to open new restaurants or have a negative impact on the Company's existing and future operations and results:

Changes in legal or regulatory requirements, including franchising laws, payment card industry rules, overtime rules, minimum wage rates, government-mandated health care benefits, tax legislation, federal ethanol policy and accounting standards, may adversely affect our ability to open new restaurants or otherwise hurt our existing and future operations and results.

Each Wendy's restaurant is subject to licensing and regulation by health, sanitation, safety and other agencies in the state and/or municipality in which the restaurant is located, as well as to Federal laws, rules and regulations and requirements of non-governmental entities such as payment card industry rules. State and local government authorities may enact laws, rules or regulations that impact restaurant operations and the cost of conducting those operations. There can be no assurance that we and/or our franchisees will not experience material difficulties or failures in obtaining the necessary licenses or approvals for new restaurants, which could delay the opening of such restaurants in the future. In addition, more stringent and varied requirements of local governmental bodies with respect to tax, zoning, land use and environmental factors could delay or prevent development of new restaurants in particular locations.

63. The foregoing clearly demonstrates the Individual Defendants' recognition of the need to abide by payment card industry rules and regulations and the grave danger that a security breach would impose upon the Company.

The Individual Defendants Knew that Wendy's was not Implementing Reasonable Measures to Secure its Customers' Data, Including Measures that were Required by its Contracts with the Payment Card Industry

64. PCI DSS are promulgated by the PCI Council. These industry requirements apply to all organizations and environments where cardholder data is stored, processed, or transmitted. The PCI Council characterizes PCI DSS as "baseline" standards that consist of "a minimum set of requirements."² In other words, a company's data security policies and procedures may be expected to exceed, but should not fall below, the minimum standards set by the PCI DSS.

65. As stated by Quick Service Restaurant ("QSR") Magazine, "The security benefits associated with maintaining PCI compliance are vital to the long-term success of all merchants who process card payments. This includes continual identification of threats and vulnerabilities

² PCI Security Standards Council LLC, PCI DSS Requirements and the Security Assessment Procedures, Version 3.1, 5 (April, 2015).

that could potentially impact the organization. Most organizations never fully recover from data breaches because the loss is greater than the data itself³.”

66. Prior to and during the time that the Data Breach occurred, the Individual Defendants knew that Wendy’s was required, pursuant to its agreements with payment card processors and networks, including Visa and MasterCard, to abide by PCI DSS to protect its customers’ personal and financial data.

67. As demonstrated below, the Company utterly failed to comply with PCI DSS, and the Board had knowledge of such failures.

68. PCI DSS applies to all organizations that store, process, or transmit payment card data. PCI DSS establishes the minimum level of protection required, not the maximum.

69. All organizations that handle payment card data are required to implement safeguards set down in the PCI DSS.

70. PCI DSS 3.1, the version of the standards in effect at the time of the Data Breach, required that Wendy’s:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access

³ https://www.pcisecuritystandards.org/pqi_security/why_security_matters

- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for employees and contractors

71. The Individual Defendants failed to ensure that Wendy’s was in compliance with the PCI DSS standards at the time of the Data Breach. Wendy’s failure to adhere to PCI DSS, as required by its agreements with payment card processors and networks, exposed the Company to potentially massive liability in the event of a data breach.

The Individual Defendants were Aware that Wendy’s Data Security Measures were Inadequate and the Company was Vulnerable to Attack

72. The Individual Defendants knew that the Company’s data security measures were inadequate, rendering the Company vulnerable to a security breach.

73. A senior engineer (“SE2”) working out of Wendy’s corporate headquarters between 2014 and 2015 who initially reported to the Chief Engineer of IT Infrastructure, Jim Gatto, and subsequently to the Director of Store Technology, Phil Newsome, described the Company’s corporate culture toward data security as a “hope for the best” attitude towards data security.⁴ FIACAC ¶¶ 81-82. SE2 stated that the Company’s IT personnel, including those in upper management, “had no clue what they were doing” and often addressed issues in ways that weakened the data security system, rather than strengthened it. FIACAC ¶ 81. SE2 also stated that there was a general lack of accountability in the Company’s IT department and IT personnel lacked both proper training and a solid understanding of how the Company’s IT systems operated. *Id.* ¶ 82. SE2 also emphasized that Wendy’s IT department routinely failed to address

⁴ The operative complaint in *First Choice Federal Credit Union, et al., v. The Wendy’s Company, et al.*, Case No.: 2:16-cv-00506 (W.D. PA) is referred to herein as the Financial Institutions’ Amended Class Action Complaint (“FIACAC”).

known security issues. For example, SE2 explained that IT management continued to use the Windows XP operating system for the Aloha POS system despite well-known vulnerabilities. Windows XP was an outdated operating system that Microsoft no longer supported with security and technical updates. *Id.* ¶ 83. When SE2 raised concerns with IT employees regarding the Company’s continued use of Windows XP, the employees would act horrified and surprised yet, nothing was ever done to rectify the problem. *Id.*

74. The high-profile data breaches at Target, Home Depot and others put the Individual Defendants on notice of the threat of a data breach. In fact, Visa warned merchants, including Wendy’s, as early as August 2013 of malware targeting POS systems. The alert, “Retail Merchants Targeted by memory-Parsing Malware,” warned: “Since January 2013, VISA has seen an increase in network intrusions involving retail merchants. Once inside the merchant’s network, the hacker will install memory parser malware on the Windows based cash register system in each lane.”⁵

75. Despite knowing the foregoing vulnerabilities, the Individual Defendants failed to implement adequate data security measures to adequately ensure that its customers’ personal and financial information was secure in compliance with the PCI DSS.

The Individual Defendants Failed to Ensure that Wendy’s Installed and Maintained an Adequate Firewall and Failed to Ensure that Payment Card Data was Segmented From the Remainder of Wendy’s Network

76. The PCI DSS required retailers to install and maintain an adequate firewall in order to prevent unauthorized persons from gaining access to systems upon which cardholder data was transmitted or stored.

77. A firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules. Acting as a barrier

⁵ <http://cybersecure.com/2013/09/10/retail-merchants-targeted-by-memory-parsing-malware-visa/>

between a trusted network and other untrusted networks (e.g., the Internet) or less-trusted networks (e.g., a retail merchant's network outside of a cardholder data environment), a firewall controls access to the resources of a network through a positive control model. This means that only traffic expressly allowed in the firewall policy is permitted onto the network; all other traffic is denied.

78. As set forth in the FIACAC, a former Wendy's employee who worked as a Field Network/System Administrator and was responsible for implementing network security upgrades at various corporate-owned and franchised restaurants confirmed that many of the restaurants he visited lacked any firewall whatsoever. *Id.* ¶ 112. The former field network/system administrator stated that other technicians also confirmed that certain Wendy's restaurants lacked any firewall. *Id.*

79. The former field network/system administrator identified problems associated with the Company's firewall configuration. *Id.* ¶ 113. As an example, when working on an upgrade project for the Company, the former field network/system administrator learned that the necessary routers had not been delivered to the restaurant sites. He advised his supervisor of the situation and stated that his supervisor told him to go to Wal-Mart to buy "any router" he could find to use in the conversion. *Id.* Although the former field network/system administrator warned his supervisor that any hacker could easily exploit this workaround and gain access to payment card data and refused to use routers purchased from Wal-Mart, he remarked that some of his colleagues did, in fact, use the inappropriate routers. *Id.* The former field network/system administrator stated that the Wal-Mart routers were not PCI DSS compliant. *Id.*

80. Pursuant to the FIACAC, Wendy's also lacked proper network segmentation to prevent a user with access to one area of the network from accessing other areas of the network

where payment card data would be stored. *Id.* ¶ 115. The former field network/system administrator stated that Wendy's maintained two (or dual) networks which were both connected to the Aloha POS system. *Id.* The former field network/system administrator further stated that dual networks lacked proper network segmentation, which would allow a hacker, who could gain access to one area of the network, to access other areas of the network to steal payment card data. *Id.* The former field network/system administrator was certain that Wendy's dual network configuration was not PCI DSS compliant because payment card data was not adequately separated from Wendy's public wireless internet network. *Id.*

81. The former field network/system administrator also stated that he was performing a network security upgrade in 2015 to render Wendy's IT environment less penetrable, specifically by improving the firewall protection and separating payment card data from Wendy's public wireless internet network. *Id.* ¶ 116. During the time of his departure from Wendy's in February 2016, the former field network/system administrator stated that there remained hundreds of Wendy's establishments that needed to perform the network security upgrade, which included proper network segmentation. *Id.* That hundreds of restaurants had inadequate data security during the time of the Data Breach clearly indicates that the Individual Defendants failed to timely implement the necessary changes and upgrades.

82. According to the FIACAC, another former Wendy's employee who worked as a senior engineer in Restaurant Infrastructure also stated that there were network segmentation issues with respect to the setup of the servers at Wendy's restaurants. *Id.* ¶ 117. He stated that all devices with electronic connectivity, including point-of-sale terminals and electronic menu board displays, resided on the same network. *Id.* Therefore, anyone who could gain access to

the network would also be able to gain access to payment card data which was, according to the senior engineer in Restaurant Infrastructure, a violation of PCI DSS. *Id.*

83. The senior engineer in Restaurant Infrastructure stated that every Wendy's restaurant that was using the Aloha POS system, regardless if it was a franchise or a company-owned store, was connected to the Aloha command center. *Id.* ¶ 118. This allowed Wendy's corporate headquarters to also have access to each restaurant running the Aloha POS system. *Id.* The Aloha Command Center also allowed the Company to monitor the status of each server and point-of-sale terminal and provide access to render technical or other support to Aloha POS system users. *Id.* The senior engineer in Restaurant Infrastructure stated that the corporate data center, which was housed on a server at the Company's headquarters, included the Aloha Command Center software that ran on all stores utilizing the Aloha POS system. *Id.* This configuration demonstrates that, absent proper network segmentation, there was full electronic connectivity between corporate and its franchisees. *Id.* As a result of this connectivity, coupled with the lack of adequate firewall protection and proper network segmentation, a hacker not only could enter Wendy's computer network, but also would be able to jump unhindered between various network platforms and ultimately access Wendy's customers' payment card data. *Id.*

84. Given that the Company's 2015 Form 10-K states that Wendy's conducts "restaurant operational audits and field visits from Company supervisors," it can be reasonably inferred that the Individual Defendants were aware that multiple restaurants did not maintain adequate data security.

The Individual Defendants Failed to Implement Protocols that Would Have Protected Payment Card Data

85. The Individual Defendants failed to implement certain protocols, such as software image hardening, password protecting programs that captured payment card data, and encrypting

payment card data at the point-of-sale, which would have detected and prevented unauthorized programs from being installed on Wendy's POS systems and otherwise would have protected payment card data in the event of a breach.

86. Hardening is the process of stripping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers. According to the FIACAC, the senior engineer in Restaurant Infrastructure was responsible for making sure that images of the software that were released and deployed to all restaurants using the Aloha POS system met PCI DSS requirements. *Id.* ¶ 120. The senior engineer in Restaurant Infrastructure was responsible for analyzing images from all of the devices in use in the restaurants, including POS terminals, kitchen devices, and back office servers – all of which were running Aloha POS software and had access to payment card data. *Id.* The senior engineer in Restaurant Infrastructure stated that if images of the software were not hardened, it could allow payment card data to be stolen from the system. *Id.* The senior engineer in Restaurant Infrastructure stated that Wendy's had not hardened the system images successfully and believed this made Wendy's vulnerable to a data breach. *Id.*

87. After the senior engineer in Restaurant Infrastructure left Wendy's and immediately before the Data Breach, the senior engineer stated that the person who assumed responsibility for ensuring that images were hardened and released was not qualified for the job and further, that his replacement would call the senior engineer nearly every day for help with the imaging process. *Id.* ¶ 121. Based on these discussions, the senior engineer in Restaurant Infrastructure knew that the images of the software were not properly hardened, which rendered the Aloha POS system vulnerable to a security breach. *Id.*

88. Another former senior engineer also confirmed that, prior to the Data Breach, none of the versions of the Aloha POS software that Wendy's was deploying were hardened. *Id.* ¶ 122.

89. Additionally, the FIACAC stated that the Company failed to encrypt payment card data at the POS terminal. *Id.* ¶ 123.

90. PCI DSS also mandated that retailers not store cardholder data any longer than necessary and encrypt any cardholder data at the point of sale so as to render any retained data unreadable to hackers.

91. Encryption is a cryptographic process by which data is encoded in such a way that only authorized parties can decrypt it. Without the proper private key, encrypted information appears as a string of undecipherable characters. Only after a user unlocks the information with her private key does it transform the data to its original, user-readable form.

92. Cardholder data is at risk of being exposed or stolen during two stages of the payment process: pre-authorization, when the merchant has captured a consumer's data and is waiting to send it to the acquirer; and post-authorization, when cardholder data has been sent back to the merchant with a response from the acquirer, and is placed into some form of storage in the merchant's servers.

93. PCI DSS explained that, even if an intruder was able to penetrate the firewall, encryption at the point of sale could still protect the data accessed and thereby reduce the risk of loss. Encryption also would protect data stored in the merchant's servers. PCI DSS made clear that, under no circumstances should unencrypted data be stored on servers or, worse, transmitted through end-user messaging technologies, such as email.

94. According to the FIACAC, the senior engineer in Restaurant Infrastructure stated that although the electronic data capture (“EDC”) file containing payment card data would be encrypted during its transfer between an Aloha POS terminal and the bank authorizing the transaction, payment card data existed in an unencrypted format on the Aloha POS terminals. *Id.* ¶ 123.

95. The senior engineer in Restaurant Infrastructure stated that the EDC file containing payment card data would be accessible remotely by anyone using the Aloha Command Center software. *Id.* ¶ 124. Additionally, he stated that the user identification and passwords associated with these EDC files were not encrypted and thus, could be stolen by hackers to unencrypt any later-encrypted payment card data. *Id.*

96. According to the FIACAC, another former senior engineer of the Company identified Wendy’s password management as another potential weakness in Wendy’s computer system. He explained that the same passwords were used across certain devices and that “any former employee with an axe to grind” could cause significant damage to Wendy’s, since Wendy’s did not regularly, if ever, change these generic passwords. *Id.* ¶ 125.

The Individual Defendants Failed to Install Software to Adequately Track and Monitor Its Network

97. Wendy’s failed to adequately track access to its network and to monitor its network for unusual activity, particularly with respect to its point-of-sale terminals, which would have allowed Wendy’s to detect and potentially prevent hackers from stealing payment card data. Symantec, one of the software vendors, provides the following with regard to this type of endpoint protection software: “Symantec’s network threat protection analyzes incoming data and blocks threats while they travel through the network before hitting endpoints. Rules-based firewall and browser protection are also included to protect against web-based attacks.” Had

Wendy's implemented proper endpoint detection and prevention systems, it would have been able to identify suspicious activity occurring within Wendy's network. Proper endpoint protection would have triggered warnings and alerted Wendy's to the transmission of payment card data within its system and should have alerted Wendy's to large volumes of data being removed, or exfiltrated, from its network.

The Individual Defendants Failed to Upgrade the Company's Systems to Utilize EMV Technology

98. Following the litany of data breaches, the payment card industry determined that it would shift to an EMV, or Chip-and-Pin, system by October 2015. U.S. merchants were given until October 1, 2015 to make the switch, and any merchant who had not made the switch before the deadline, such as Wendy's, would now be liable for payment fraud caused by compromised POS terminals.

99. EMV cards, which have a secret algorithm embedded in a chip that creates a unique transaction code that cannot be used again, are designed to be far more expensive and difficult for thieves to counterfeit. By contrast, the traditional non-chip cards store unchanging data on a magnetic strip, which can be easily copied and re-encoded onto virtually anything else with a magnetic strip. Indeed, magnetic strip cards were the primary target for hackers who broke into Target and Home Depot and installed malicious software on the cash registers.

100. Yet, despite the regulatory changes requiring merchants to switch to EMV technology, the Individual Defendants failed to do so and in fact, never had plans to make the transition. During a conference that took place in 2013, Gavin Waugh, vice president and treasurer at Wendy's, stated "[Wendy's] actual fraud rate is so small it's hardly worth mentioning. [EMV] doesn't move the needle that much. Even if we pay the fraud liability, it's a whole lot cheaper than putting in [EMV] terminals." The hamburger chain processes 300,000

card transactions daily, Waugh said. Waugh also noted that the implementation of EMV technology would cost a “staggering amount of money.” Ironically during the same conference, the merchant panel, including Waugh, acknowledged that “EMV tackles only point-of-sale fraud⁶.”

101. To make matters even worse, after the Company confirmed the Data Breach, Waugh declined to say whether Wendy’s has a timetable for deploying chip-based readers in its restaurants, but stated “I don’t think that would have solved this problem, and it’s a bit of a misnomer . . . I think it makes it harder [for the attackers], but I don’t think it makes it impossible.”

102. Had the Individual Defendants taken the proper steps to implement EMV technology, the Data Breach could have been prevented or, at the very least, mitigated. Yet, despite the fact that the payment card industry set a deadline of October 1, 2015 for businesses to transition their systems from magnetic-strip to EMV technology, the Individual Defendants, in conscious disregard of their fiduciary duties, failed to comply with that deadline.

The Data Breach and the Individual Defendants’ Inadequate Response

103. On January 27, 2016, security blogger Brian Krebs of *KrebsonSecurity* first broke the news that Wendy’s was investigating claims of a possible credit card breach at some locations. The acknowledgment from the Company came in response to questions from *KrebsonSecurity* about banking industry sources who discovered a pattern of fraud on cards that were all recently used at various Wendy’s locations.

104. Bob Bertini, Wendy’s spokesperson, told Krebs that Wendy’s “received this month from [the Company’s] payment industry contacts reports of unusual activity involving

⁶ <http://www.digitaltransactions.net/index.php/news/story/Execs-with-Major-Retailers-Complain-EMV-Attacks-Wrong-Problem-at-Huge-Expense>

payment cards at some of [Wendy's] restaurant locations. Reports indicate that fraudulent charges may have occurred elsewhere after the cards were legitimately used at some of [the Company's] restaurants. [Wendy's has] hired a cybersecurity firm and launched a comprehensive and active investigation that's underway to try to determine the facts."

105. Although Bertini said that it was too soon to say whether the incident is contained, how long it may have persisted or how many stores may be affected, Bertini stated that the Company "began investigating immediately, and the period of time [the Company] is looking at the incidents is late last year."

106. On February 9, 2016, the Company filed a current report on Form 8-K and an accompanying press release with the SEC announcing its preliminary results for the fourth quarter and full year ended January 3, 2016. In the press release, the Company provided the following update on its investigation:

Update on Investigation into Unusual Credit Card Activity

As reported in the news media in late January, the Company has engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity related to certain Wendy's restaurants. Out of the locations investigated to date, some have been found by the cybersecurity experts to have malware on their systems. The investigation is ongoing, and the Company is continuing to work closely with cybersecurity experts and law enforcement officials.

107. On March 2, 2016, Krebs reported that a number of credit unions have stated that they have experienced an "unusually high level of debit card fraud from the breach at [] Wendy's, and that the *losses so far eclipse those that came in the wake of huge card breaches at Target and Home Depot.*" (Emphasis added).

108. Krebs stated that after speaking with a bank security consultant who was helping several financial institutions deal with the fallout from the Wendy's breach, the consultant stated that many of the banks had customers who re-compromised their cards several times in one

month because they ate at several different Wendy's locations throughout the month. Krebs further reported that although many banks and credit unions are now issuing more secure chip-based credit and debit cards (which are designed to make it more difficult and more expensive for thieves to counterfeit stolen cards), it appears that the breached Wendy's locations were not asking customers to "dip their chip cards but instead swipe the card's magnetic strip," thus confirming that Wendy's had not yet transitioned to utilizing EMV technology in its restaurants, despite the October 2015 deadline.

109. The next day on March 3, 2016, the Company filed its annual report on Form 10-K with the SEC (the "2015 10-K") providing the following update on the Company's investigation, in relevant part:

As reported in the news media in late January, the Company has engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity at some Wendy's restaurants. Out of the locations investigated to date, some have been found by the cybersecurity experts to have malware on a certain system. The investigation is ongoing and the Company is continuing to work closely with cybersecurity experts and law enforcement officials.

110. On May 11, 2016, the Company filed a quarterly report on Form 10-Q with the SEC reporting the Company's financial results for the three months ended April 3, 2016 (the "2016 1Q 10-Q"). In the 2016 1Q 10-Q, the Company provided the following update on the breach:

Certain of Our Franchisees have Experienced a Data Incident

Earlier this year, the Company engaged cybersecurity experts to conduct a comprehensive investigation into unusual credit card activity at some Wendy's restaurants. Investigation into this activity is nearing completion. Based on the preliminary findings of the investigation and other information, the Company believes that malware, installed through the use of compromised third-party vendor credentials, affected one particular point of sale system ***at fewer than 300 of approximately 5,500 franchised North America Wendy's restaurants, starting in the fall of 2015.*** These findings also indicate that ***the Aloha point of sale system has not been impacted by this activity.*** The Aloha system is already installed at all Company-owned restaurants and in a majority of franchise-owned

restaurants, with implementation throughout the North America system targeted by year-end 2016. The Company expects that it will receive a final report from its investigator in the near future.

The Company has worked aggressively with its investigator to identify the source of the malware and quantify the extent of the malicious cyber-attacks, and has ***disabled and eradicated the malware in affected restaurants***. The Company continues to work through a defined process with the payment card brands, its investigator and federal law enforcement authorities to complete the investigation. Based upon the investigation to date, ***approximately 50 franchise restaurants are suspected of experiencing, or have been found to have, unrelated cybersecurity issues***. The Company and affected franchisees are working to verify and resolve these issues.

The Company has been named as a defendant in two putative class actions filed in the United States on behalf of customers and payment card issuing banks seeking damages and other relief allegedly arising from the data incident. In addition, claims may also be made by payment card networks against the affected franchisees. These claims and investigations may adversely affect how we or our franchisees operate the business, divert the attention of management from the operation of the business, have an adverse effect on our reputation, result in additional costs, and adversely affect our results of operations.

(Emphasis added).

111. Based on the foregoing, the Company confirmed that the Data Breach began in the fall of 2015, thus evidencing that the Data Breach went undetected for months. To make matters worse, the Company only learned of the Data Breach after banking industry sources advised security blogger Brian Krebs that they discovered a pattern of fraud on cards that were recently used at Wendy's locations. Moreover, despite the statements by the Company that the Data Breach was limited in scope, had been contained and had not affected the Aloha POS system, in reality, the exact opposite was true.

112. On June 9, 2016, the Company filed a current report on Form 8-K along with an accompanying press release with the SEC announcing that it had recently discovered a second strain of malware at additional restaurants that had affected a POS system that the Company

previously believed had not been impacted. The press release stated the following, in relevant part:

WENDY'S UPDATE ON UNUSUAL CREDIT CARD ACTIVITY

Company Disables Malware Discovered at Additional Restaurants

DUBLIN, Ohio, June 9, 2016 –The Wendy's Company (NASDAQ: WEN) announced today that *additional malicious cyber activity has recently been discovered in some franchise-operated restaurants. The Company has disabled the malware where it has been detected.*

This latest action is the result of the Company's continuing investigation into unusual credit card activity at some Wendy's® restaurants. Reports indicate that payment cards used legitimately at Wendy's may have been used fraudulently elsewhere.

Based on the preliminary findings of the previously-disclosed investigation, the Company reported on May 11 that malware had been discovered on the point of sale (POS) system at fewer than 300 franchised North America Wendy's restaurants. An additional 50 franchise restaurants were also suspected of experiencing, or had been found to have, other cybersecurity issues. As a result of these issues, the Company directed its investigator to continue to investigate.

In this continued investigation, *the Company has recently discovered a variant of the malware, similar in nature to the original, but different in its execution. The attackers used a remote access tool to target a POS system that, as of the May 11th announcement, the Company believed had not been affected.* This malware has been discovered on some franchise restaurants' POS systems, and the number of franchise restaurants impacted by these cybersecurity attacks is now *expected to be considerably higher than the 300 restaurants already implicated.* To date, there has been no indication in the ongoing investigation that any Company-operated restaurants were impacted by this activity.

Many franchisees and operators throughout the retail and restaurant industries contract with third-party service providers to maintain and support their POS systems. The Company believes this series of cybersecurity attacks resulted from *certain service providers' remote access credentials being compromised, allowing access to the POS system in certain franchise restaurants serviced by those providers.*

The malware used by attackers is highly sophisticated in nature and extremely difficult to detect. Upon detecting the new variant of malware in recent days, the Company has already disabled it in all franchise restaurants where it has been

discovered, and the Company continues to work aggressively with its experts and federal law enforcement to continue its investigation.

(Emphasis added).

113. As set forth in the Amended Complaint in the Consumer Class Action, the foregoing press release contained numerous material omissions, including but not limited to, the following:

- 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 this threat was ongoing.

ACCAC ¶ 57.⁷

114. Later that same day, Krebs reported about the Data Breach, noting that the Company's most recent statement that "the attackers got access by stealing credentials that allowed remote access to point-of-sale terminals should hardly be surprising: The vast majority of the breaches involving restaurant and hospitality chains over the past few years have been tied to hacked remote access accounts that POS service providers use to remotely manage the devices."

115. Krebs also remarked that "many retailers are now moving to install card readers that can handle transactions from more secure chip-based credit and debit cards, which are far more expensive for thieves to clone." Gavin Waugh, vice president and treasurer at Wendy's,

^{7 7} The operative complaint in *Torres, et al. v. Wendy's International LLC*, Case No.: 6:16-cv-210 (M.D. Fla.) is referred to herein as the Amended Consumer Class Action Complaint ("ACCAC").

declined to say whether Wendy's has a timetable for deploying chip-based readers in its restaurants, but stated "I don't think that would have solved this problem, and it's a bit of a misnomer . . . I think it makes it harder [for the attackers], but I don't think it makes it impossible."

116. These statements hardly come as a surprise, given Waugh's prior comments indicating that the cost of installing EMV technology greatly outweighs the benefits. Indeed, during a conference that took place in 2013, Waugh stated "[Wendy's] actual fraud rate is so small it's hardly worth mentioning. [EMV] doesn't move the needle that much. Even if we pay the fraud liability, it's a whole lot cheaper than putting in [EMV] terminals." The hamburger chain processes 300,000 card transactions daily, Waugh said. Waugh also noted that the implementation of EMV technology would cost a "staggering amount of money." Ironically during the same conference, the merchant panel, including Waugh, acknowledged that "EMV tackles only point-of-sale fraud⁸."

117. Had the Individual Defendants taken the proper steps to implement EMV technology, the Data Breach could have been prevented or, at the very least, mitigated. Yet, despite the fact that the payment card industry set a deadline of October 1, 2015, for businesses to transition their systems from magnetic-strip to EMV technology, the Individual Defendants, in conscious disregard of their fiduciary duties, failed to comply with that deadline.

118. On July 7, 2016, the Company issued a news release on its website which provided the following update on the Company's investigation into the breach, in relevant part:

⁸ <http://www.digitaltransactions.net/index.php/news/story/Execs-with-Major-Retailers-Complain-EMV-Attacks-Wrong-Problem-at-Huge-Expense>

Wendy's Update on Payment Card Security Incident

Customers Now Able to Access More Specific Information About Potentially Impacted Locations on Website – Company Offers Complimentary Fraud Consultation and Identity Restoration Services

DUBLIN, Ohio, July 7, 2016 /PRNewswire/ -- The Wendy's Company (NASDAQ: WEN) updated its customers today regarding malicious cyber activity experienced at some Wendy's® restaurants. The Company first reported unusual payment card activity affecting some franchise-owned restaurants in February 2016. Subsequently, on June 9, 2016, the Company reported that an additional malware variant had been identified and disabled. Today, the Company, on behalf of affected franchise locations, is providing information about specific restaurant locations that may have been impacted by these attacks, all of which are located in the U.S., along with support for customers who may have been affected by the malware variants.

"We are committed to protecting our customers and keeping them informed. We sincerely apologize to anyone who has been inconvenienced as a result of these highly sophisticated, criminal cyberattacks involving some Wendy's restaurants," said Todd Penegor, President and Chief Executive Officer. "We have conducted a rigorous investigation to understand what has occurred and apply those learnings to further strengthen our data security measures."

Wendy's customers are encouraged to learn more about this new information at the following address: www.wendys.com/notice. The update includes a list of restaurant locations that may have been involved in the incidents, as well as information on how customers can protect their credit and details regarding how potentially affected customers can receive one year of complimentary fraud consultation and identity restoration services. A link to the update can also be found on the Company's homepage, www.wendys.com.

Working closely with third-party forensic experts, federal law enforcement and payment card industry contacts as part of its ongoing investigation, the Company has determined that specific payment card information was targeted by the additional malware variant. ***This information included cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code.***

Generally, individuals that report unauthorized charges in a timely manner to the bank or credit card company that issued their card are not responsible for those charges. As always, in line with prudent personal financial management, we encourage our customers to be diligent in watching for unauthorized charges on their payment cards.

The Company believes the criminal cyberattacks resulted from service providers' remote access credentials being compromised, allowing access – and the ability to deploy malware – to some franchisees' point-of-sale systems. To date, there has been no indication in the ongoing investigation that any Company-operated restaurants were impacted by this activity.

The Company worked with investigators to disable the malware involved in the first attack earlier this year. Soon after detecting the malware variant involved in the latest attack, the Company identified a method of disabling it and thereafter disabled it in all franchisee restaurants where it was discovered. *The investigation has confirmed that criminals used malware believed to have been effectively deployed on some Wendy's franchisee systems starting in late fall 2015.*

(Emphasis added).

119. Despite representing to the public that more information about the Data Breach was available on the Company's website, Wendy's failed to provide any additional information and what little information it did provide was inadequate and redundant. Indeed, the Individual Defendants have continued to remain silent about the specifics of the Data Breach and the status of the Company's investigation.

120. Noticeably absent from the Company's June 9, 2016 press release or Wendy's July 7, 2016 news release, and contrary to the Company's earlier public disclosures, was the representation that none of the Aloha POS systems had been compromised. Indeed, to this day, the Company has failed to acknowledge that the Aloha POS system that Wendy's required its franchisees to install had also been involved in the Data Breach.

The Individual Defendants Knew that the Company's Aloha POS System was Inadequate and Would Not Protect Against a Data Breach

121. Prior to the Data Breach, the Individual Defendants were aware that its data security systems were insufficient and outdated that its POS system would not protect the Company against a data breach.

122. On December 22, 2014, Wendy's filed a lawsuit against DavCo Restaurants LLC and DavCo Acquisition Holding, Inc. (collectively "DavCo"), one of the Company's largest

franchisees⁹, seeking to immediately terminate each of DavCo's franchise agreements on the grounds of DavCo's alleged failure to comply with the terms of the franchise agreements by not, among other things, purchasing and installing, a common point of sale computer platform.

123. According to Wendy's complaint against DavCo ("DavCo Complaint"), "in October 2012, Wendy's formally announced plans to implement NCR Aloha ("Aloha") as the required POS platform for the Wendy's system in the U.S. and Canada." DavCo Complaint ¶ 16. Further, Wendy's admitted that this was a significant and important announcement, as prior to this time, Wendy's remained one of the few major quick-service restaurant chains that had not yet implemented a single, consistent POS platform system wide. *Id.* The DavCo Complaint also stated that "NCR is a publicly-traded, leading provider of technology solutions and Aloha is regarded as one of the best, if not the best, POS solutions available to the restaurant industry," *id.*, and that Wendy's selected Aloha following a lengthy, in-depth selection process managed by Wendy's IT and Operations departments, with continuous input from Wendy's U.S. and Canadian franchise advisory councils, whose members are comprised of franchisees representing multiple geographic regions within the U.S. and Canada. *Id.* ¶ 18.

124. Indeed, in an exchange between defendant Brolick and an analyst from CL King & Associates, Inc. that took place during the 2012 4Q Earnings Call,¹⁰ defendant Brolick admitted that the Company's POS system was outdated and that the Company would need to move fairly quickly to adopt the Aloha POS system:

Analyst: Okay, great. And then just a follow-up question. I guess when you look at the remodels, I assume as stores get done, you're going to get everybody on a common POS platform. I was wondering just how long you think it'll take to get the system on a -- more of a common POS platform so you can better utilize the

⁹ The lawsuit is captioned as *Wendy's Int'l, LLC v. DavCo Rests. LLC*, No. 14CV013382 (Ohio Ct. Comm. Pl.) (the "DavCo Lawsuit")

¹⁰ <http://seekingalpha.com/article/1234861-the-wendys-management-discusses-q4-2012-results-earnings-call-transcript?part=single>

new app and be able to really utilize some of the tools that hit those customers more efficiently from a marketing standpoint.

Brolick: Yes. Well, I'll start out and then ask Steve to jump in here. But *there is a fairly high percentage of our system that has fairly old POS software*, and they're going to need to evolve to this fairly quickly. There are also franchisees, however, who have quite recently made important investments in what we call modern POS hardware as well as software. They will eventually have to transition out of that into the common platform that we have identified, which is NCR's Aloha. But that might be 5 years down the road for them. But again, they have modern POS that can run this. So that's not an issue. But to do the things we want longer term, there -- they, too, are eventually going to have to change. But there's a decent piece of the system that's going to have to move to this really pretty quickly.

(Emphasis added).

125. Further, despite Brolick's acknowledgment that the Company's systems were outdated and that the transition to Aloha POS would have to happen quickly, although the original deadline to install Aloha in all Wendy's restaurants was July 1, 2014, Wendy's claimed that it extended the deadline to July 1, 2015 "in order to give Wendy's franchisees additional time to plan for and make the recurring investment to help ensure a successful rollout of Aloha in all restaurants." DavCo Complaint ¶ 19.

126. On February 16, 2015, DavCo filed its answer to the complaint and asserted counterclaims against Wendy's (the "DavCo Counterclaim"). The DavCo Counterclaim alleged that the Aloha POS system was fraught with serious technical and operational problems which, according to DavCo, Wendy's acknowledged, but summarily dismissed as trivial. DavCo Counterclaim ¶ 9. DavCo further alleged that the Aloha POS software was unstable and would repeatedly freeze and disconnect from the restaurant's network, causing Wendy's to temporarily suspend Aloha installations in late 2013 because of concerns relating to the software's stability. *Id.* ¶¶ 25-30.

127. On June 30, 2016, after Wendy's had confirmed the Data Breach, Wendy's filed its first amended complaint against DavCo and on July 15, 2016, DavCo filed its first amended answer and asserted counterclaims against Wendy's (the "DavCo Amended Counterclaim").

128. The DavCo Amended Counterclaim stated that DavCo determined in 2005 and 2006 to modernize its POS system and, after consulting with John Deane, Wendy's Chief Information Officer at the time, Mr. Deane recommended the Micros POS system as the most suitable for a Wendy's franchise. DavCo Amended Counterclaim at ¶ 26. Additionally, Mr. Deane stated that Wendy's itself would be adopting the Micros POS system for use in Company owned restaurants. *Id.*

129. The DavCo Amended Counterclaim went on to state that although the Company's information technology department reviewed multiple POS systems in 2005 and 2006, including the Aloha POS system, Wendy's rejected Aloha for use in its company-owned restaurants at the time. *Id.* ¶ 27.

130. With respect to the Aloha POS System, the DavCo Amended Counterclaim alleges that "the frequent problems demonstrated by Wendy's poor decision to adopt the Aloha POS system is exhibited by the ever-changing deadlines cited in Wendy's complaints in this litigation. Wendy's selected the Aloha platform in October 2012 – nearly four years ago. Wendy's then decided upon an original deadline of July 1, 2014 to install Aloha. Because of major problems with Aloha, that deadline was eventually delayed to July 1, 2015. Now Wendy's claims that the deadline was March 31, 2016, though not all restaurants are required to have the Aloha system installed until at least December 31, 2016. Upon information and belief, it is unlikely that this latest announced deadline will be met. And some Wendy's restaurants will never have to install the Aloha system." DavCo Amended Counterclaim ¶ 11.

131. Further, DavCo alleged that “the functional capacity of the Aloha system was also subject to ridicule among franchisees” and that Wendy’s informed its franchisees on November 18, 2014 that the problems with the Aloha POS system “were ‘causing more disruption than we would consider to be reasonable.’” *Id.* ¶ 29.

132. The DavCo Amended Counterclaim also included the following allegations about the Data Breach, in relevant part:

Upon information and belief, there continue to be significant problems with the Aloha POS system. In January 2016, reports disclosed a possible data breach arising from Wendy’s POS systems. Wendy’s confirmed in May 2016 that franchisee POS systems were the target of a consumer data breach, but stated that the breach affected only around 300 restaurants and that Aloha was not affected. However, in June 2016, Wendy’s revealed that the data breach was larger and may have affected another POS system without disclosing what system specifically. On July 7, 2016, Wendy’s disclosed that the data breach occurred over the course of two waves and affected over 1,000 restaurants – nearly 20% of Wendy’s franchise locations in the United States. ***Upon information and belief, many of the affected restaurants utilized the Aloha POS system.*** None of DavCo’s restaurants – which have not installed the Aloha system to date – appear to have been affected by the data breach. Despite not having any restaurants which were part of the data breach suffered by those franchised restaurants that installed the Aloha POS system, DavCo has been subjected to numerous media reports and suspicion from its customers that their data may have been compromised as part of the Aloha data breach.

Id. ¶ 34 (Emphasis added).

133. Further, the DavCo Amended Counterclaim stated that Don Zimmerman served as Wendy’s Chief Information Officer from 2008 to 2015 and that he was primarily responsible for deciding the technology vendors that would service Wendy’s restaurants including NCR, the developer of the Aloha POS system. *Id.* ¶ 35. DavCo claimed that Mr. Zimmerman played a “crucial role” in deciding that the Aloha POS system would be required for use in Wendy’s restaurants despite its many flaws and, notably, after Zimmerman’s departure from Wendy’s in 2015, he went on to become the Chief Technology Officer for NCR’s hospitality division. *Id.*

134. On July 25, 2016, Wendy's filed a reply to DavCo's Amended Counterclaim ("Wendy's Reply"). Notably, despite its prior public statements to the contrary, Wendy's did not deny DavCo's claims that the Data Breach had indeed affected restaurants that were utilizing the Aloha POS system (Wendy's Reply ¶ 34) and also admitted that Don Zimmerman was Wendy's former Chief Investment Officer, he participated in the decision to implement the Aloha POS system for the Wendy's system in the United States and Canada and Mr. Zimmerman no longer works for the Company. *Id.* ¶ 35.

135. Moreover, on July 13, 2016, Wendy's posted a job listing on its website seeking an analyst – POS solutions. Under the section of the listing entitled "Job description," the description provided by Wendy's admitted that the Aloha POS system suffered from defects, stating the following, in relevant part:

This position is responsible for assisting in supporting and enhancing Aloha application software within the Restaurant Solutions environment, and for all integrated Aloha software required for optimal restaurant operations. This role will execute *first level investigation into reported defects within new and existing Aloha POS software code and submit initial findings for further analysis and root cause determination*. This role will facilitate data gathering and requirements definitions for appropriate internal groups to better manage Third Party vendors and to ensure quality software delivery to restaurants required for optimal operations. Reporting to the Manager - Application Engineering¹¹.

(Emphasis added).

136. Based on the foregoing, despite having knowledge of the multiple problems with the Aloha POS system dating back several years and recognizing the importance of maintaining adequate data security policies and procedures, the Individual Defendants, in conscious disregard of their fiduciary duties, failed to take adequate steps to update its POS system and/or rectify the

¹¹ See https://wendys.taleo.net/careersection/ext_noncrew/jobdetail.ftl?job=PR%200002562&lang=en and <https://www.linkedin.com/jobs/view/176518237>

existing issues with the Aloha POS system, all of which could have prevented the Data Breach from occurring. This is even more egregious given that after the Company learned that the Data Breach impacted restaurants utilizing the Aloha POS system, the Company continues to utilize the faulty Aloha POS system in its restaurants and continues to require franchisees to implement the Aloha POS system in their restaurants

DAMAGES TO WENDY'S CAUSED BY THE INDIVIDUAL DEFENDANTS

137. As a direct and proximate result of the Individual Defendants' misconduct, Wendy's failed to maintain proper internal controls, consciously disregarded multiple red flags alerting the Individual Defendants to multiple areas of non-compliance with the Company's existing policies and procedures and problems with the Aloha POS system, caused the Company to release false and misleading statements and substantially damaged the Company's credibility, corporate image and goodwill.

138. Wendy's has expended and will continue to expend significant sums of money. Additional expenditures and damages that the Company has incurred as a result of the Individual Defendants' breaches of their fiduciary duty include:

- a. Costs incurred from investigating, defending and payment of any settlement or judgment in the Financial Institution Class Action and the Consumer Class Action;
- b. Costs incurred from retaining cybersecurity experts to conduct a comprehensive investigation into the Data Breach;
- c. Costs incurred in strengthening and/or implementing changes to Wendy's existing data security systems; and

- d. Costs incurred from the loss of Wendy's customers' confidence in the Company's services resulting in lost sales.

DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS

139. Plaintiff brings this action derivatively in the right and for the benefit of Wendy's to redress injuries suffered, and to be suffered, by Wendy's as a direct result of breaches of fiduciary duty and unjust enrichment.

140. Plaintiff is a shareholder of Wendy's, was a shareholder of Wendy's at the time of the wrongdoing alleged herein, and has been a shareholder of Wendy's continuously since that time.

141. Plaintiff will adequately and fairly represent the interests of the Company and its shareholders in enforcing and prosecuting its rights.

142. Wendy's is named as a nominal defendant in this case solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have. Prosecution of this action, independent of the current Board of Directors, is in the best interests of the Company.

143. The wrongful acts complained of herein subject, and will continue to subject, Wendy's to continuing harm because the adverse consequences of the actions are still in effect and ongoing.

144. The wrongful acts complained of herein were unlawfully concealed from Wendy's shareholders.

145. Throughout the Relevant Period, the Individual Defendants failed to make full and fair disclosure about the effectiveness of Wendy's internal controls and violated multiple

corporate governance principles, thus representing evidence of the Individual Defendants' breaches of fiduciary duties.

146. As a result of the facts set forth herein, Plaintiff has not made any demand on the Current Director Defendants to institute this action since demand would be a futile and useless act because the Current Director Defendants are incapable of making an independent and disinterested decision to institute and vigorously prosecute this action. The wrongful acts complained of herein show multiple breaches by the Individual Defendants, including the Current Director Defendants, of their fiduciary duties of loyalty, due care and oversight.

147. A majority of the Board is incapable of disinterestedly and independently considering a demand to commence and vigorously prosecute this action for the reasons set forth above and below.

148. As of the date of this Complaint, the Current Board consists of the following eleven individuals: defendants N. Peltz, May, Brolick, Hill, Kass, Levato, Mathews-Spradlin, M. Peltz, Penegor and Rothschild and non-defendant Arthur B. Winkleblack ("Winkleblack").

149. As an initial matter, demand upon the Current Director Defendants is futile because the Board is already predisposed to refuse a demand as demonstrated by the Current Director Defendants' position on the merits of the Financial Institutions' Class Action and Consumer Class Action, whose allegations also form the basis, in part, of liability in the instant litigation. In a Form 10-Q filed with the SEC on August 10, 2016, the Company stated the following, in relevant part:

The Company was named as a defendant in a civil complaint that was filed in the U.S. District Court for the Middle District of Florida on February 8, 2016 by plaintiff Jonathan Torres. The complaint asserted claims of breach of implied contract, negligence and violations of the Florida Unfair and Deceptive Trade Practices Act arising from the Company's alleged failure to safeguard customer credit card information and the alleged failure to provide notice that credit card

information had been compromised. The complaint sought certification of a putative nationwide class of consumers impacted by the alleged failures. The plaintiff sought monetary damages, injunctive and equitable relief, attorneys' fees and other costs. The Company's motion to dismiss the complaint was granted, without prejudice, on July 15, 2016.

An amended complaint was filed in the same court by plaintiff Jonathan Torres and six additional named plaintiffs on July 29, 2016. The amended complaint names the Company's subsidiary, Wendy's International, LLC ("Wendy's International"), as the defendant and asserts claims of breach of implied contract, negligence and violations of state consumer protection or deceptive trade practices statutes in the states of Florida, New York, New Jersey, Mississippi, Tennessee and Texas arising from Wendy's International's alleged failure to safeguard customer credit card information and the alleged failure to provide notice that credit card information had been compromised. The amended complaint also asserts violations of state data breach statutes in Florida, New York, New Jersey, Tennessee and Texas based on Wendy's International's alleged failure to timely and fully disclose the alleged data breach. The amended complaint seeks certification of a putative nationwide class of consumers impacted by the alleged failures, or in the alternative, statewide classes for Florida, New York, New Jersey, Mississippi, Tennessee and Texas. The plaintiffs seek monetary damages, injunctive and equitable relief, attorneys' fees and other costs.

The Company was named as a defendant in a civil complaint that was filed in the U.S. District Court for the Western District of Pennsylvania on April 25, 2016 by plaintiff First Choice Federal Credit Union. The complaint asserts claims of common law negligence, negligence per se due to the alleged violation of section 5 of the Federal Trade Commission Act, and declaratory and injunctive relief. All of these claims are based on the allegations arising from the Company's alleged failure to safeguard customer credit card information and the alleged failure to provide notice that credit card information had been compromised. The complaint sought certification of a putative nationwide class of banks, credit unions, financial institutions and other entities in the United States impacted by the alleged failures. The plaintiff sought monetary damages, a declaratory judgment, injunctive relief, attorneys' fees and other costs.

The Company was named as a defendant in four other civil complaints filed by financial institutions in the U.S. District Court for the Western District of Pennsylvania based on the allegations arising from the Company's alleged failure to safeguard customer credit card information and the alleged failure to provide notice that credit card information had been compromised. These cases were consolidated into the First Choice Federal Credit Union case.

An amended civil complaint was filed in the consolidated proceeding in the U.S. District Court for the Western District of Pennsylvania on July 22, 2016 naming

the Company and two of its subsidiaries as defendants. The amended complaint was brought by 22 financial institutions and five association plaintiffs (representing members who are credit unions and other similar financial institutions). The amended complaint asserts claims of common law negligence, negligence per se due to the alleged violation of section 5 of the Federal Trade Commission Act, violation of the Ohio Deceptive Trade Practices Act, and declaratory and injunctive relief. The amended complaint also seeks certification of a putative nationwide class of banks, credit unions, financial institutions and other entities in the United States impacted by the alleged failures. The plaintiffs seek monetary damages, a declaratory judgment, injunctive relief, attorneys' fees and other costs.

The Company believes it has meritorious defenses to each of the actions described above and intends to vigorously oppose the claims asserted in each of the complaints.

(Emphasis added).

150. Thus, because the Board has already determined that it believes that the allegations in the Financial Institutions' Class Action and Consumer Class Action are without merit, and because the instant action is substantially based on the same and/or similar misconduct as the Financial Institutions' Class Action and Consumer Class Action, the Current Director Defendants are incapable of making an independent and disinterested decision to institute and vigorously prosecute this derivative action.

151. Additionally, as discussed above, during the 2012 4Q Earnings Call, defendant Brolick admitted that the Company's POS system was outdated, stating "[b]ut there is a fairly high percentage of our system that has fairly old POS software, and they're going to need to evolve to this fairly quickly. There are also franchisees, however, who have quite recently made important investments in what we call modern POS hardware as well as software. They will eventually have to transition out of that into the common platform that we have identified, which is NCR's Aloha. But that might be 5 years down the road for them. But again, they have modern POS that can run this. So that's not an issue. But to do the things we want longer term,

there -- they, too, are eventually going to have to change. But there's a decent piece of the system that's going to have to move to this really pretty quickly.”

152. Based on the foregoing, defendants N. Peltz, May, Brolick, Hill, Levato and Rothschild¹², six out of the eleven Current Director Defendants, knew that the Company's POS system was outdated and inadequate and breached their fiduciary duties by failing to take timely action to update the POS system and ensure that it was PCI DSS compliant. As such, a majority of the Current Director Defendants face a substantial likelihood of liability rendering demand upon them as futile.

153. Further, a majority of the Current Director Defendants have deep-rooted longstanding relationships with each other, thus rendering demand upon them as futile.

Trian Partners and Triangle

154. With respect to defendants N. Peltz, May, Kass, Levato, and M. Peltz, pursuant to the 2016 Proxy, each of the foregoing Current Director Defendants are/were employed by and/or affiliated with each other in the following ways: (i) defendant N. Peltz has served as CEO and founding partner of Trian Partners since November 2005, from January 1989 to April 1993, N. Peltz was Chairman and CEO of Trian Group, Limited Partnership, which provided investment banking and management services for entities controlled by N. Peltz and defendant May, and from 1983 to December 1988, N. Peltz was Chairman and CEO and a director of Triangle; (ii) defendant May has been President and a founding partner of Trian Partners since November 2005, from January 1989 to April 1993, May was President and COO of Trian Group, Limited Partnership, and from 1983 to December 1988, he was President and COO and a director of Triangle; (iii) defendant Kass currently serves as an Advisory Partner of Trian

¹² Defendants Peltz, May, Brolick, Hill, Levato and Rothschild were all serving on the Board during the time of the 2012 4Q Earnings Call.

Partners; (iv) defendant Levato was Senior Vice President and Chief Financial Officer of Trian Group, Limited Partnership, from January 1992 to April 1993 and From 1984 to December 1988, Levato served as Senior Vice President and CFO of Triangle; and (v) defendant M. Peltz is a Partner and has been a member of the Investment Team of Trian Partners and is the son of defendant N. Peltz. Therefore, given their longstanding deep rooted ties to each other, defendants N. Peltz, May, Kass, Levato and M. Peltz are incapable of independently considering a demand to bring suit against one another and accordingly, demand is futile.

155. With respect to Peltz and May, according to the 2016 Proxy, as of March 28, 2016, Trian Partners was the beneficial owner of 40,792,537 (15.3%) shares of Wendy's common stock. As set forth in the Company's 2015 10-K under the section entitled "Risk Factors," Wendy's concedes that its Board is controlled by Current Director Defendants Peltz and May, who both beneficially own more than 20% of the outstanding shares of Wendy's common stock:

A substantial amount of the Company's Common Stock is concentrated in the hands of certain stockholders.

Nelson Peltz, the Company's Chairman and former Chief Executive Officer, Peter May, the Company's Vice Chairman and former President and Chief Operating Officer, and Edward Garden, who resigned as a director of the Company on December 14, 2015, beneficially own shares of the Company's outstanding Common Stock that collectively constitute more than 20% of its total voting power as of February 29, 2016. Messrs. Peltz, May and Garden may, from time to time, acquire beneficial ownership of additional shares of Common Stock.

On December 1, 2011, the Company entered into an agreement (the "Trian Agreement") with Messrs. Peltz, May and Garden, and several of their affiliates (the "Covered Persons"). Pursuant to the Trian Agreement, the Board of Directors, including a majority of the independent directors, approved, for purposes of Section 203 of the Delaware General Corporation Law ("Section 203"), the Covered Persons becoming the owners (as defined in Section 203(c)(9) of the DGCL) of or acquiring an aggregate of up to (and including), but not more than, 32.5% (subject to certain adjustments set forth in the Agreement) of the outstanding shares of the Company's Common Stock, such that no such persons

would be subject to the restrictions set forth in Section 203 solely as a result of such ownership (such approval, the “Section 203 Approval”).

The Trian Agreement (other than the provisions relating to the Section 203 Approval and certain miscellaneous provisions that survive the termination of the agreement) terminated pursuant to the termination provisions of the Trian Agreement after funds affiliated with the Covered Persons sold 16.2 million shares of the Company’s Common Stock on January 15, 2014, thereby decreasing the Covered Persons’ beneficial ownership to less than 25% of the outstanding voting power of the Company as of that date. The Covered Persons sold an additional 2.0 million shares of the Company’s Common Stock on February 25, 2014. On July 17, 2015, the Company repurchased 18.4 million shares of the Company’s Common Stock from the Covered Persons. The terminated provisions of the Trian Agreement included provisions restricting the Covered Persons in the following areas: (i) beneficial ownership of Company voting securities; (ii) solicitation of proxies or submission of a proposal for the vote of stockholders under certain circumstances; (iii) certain affiliate transactions with the Company; and (iv) voting of certain Company voting securities.

This concentration of ownership gives Messrs. Peltz, May and Garden significant influence over the outcome of actions requiring stockholder approval, including the election of directors and the approval of mergers, consolidations and the sale of all or substantially all of the Company’s assets. They are also in a position to have significant influence to prevent or cause a change in control of the Company. If in the future Messrs. Peltz, May and Garden were to acquire more than a majority of the Company’s outstanding voting power, they would be able to determine the outcome of the election of members of the Board of Directors and the outcome of corporate actions requiring majority stockholder approval, including mergers, consolidations and the sale of all or substantially all of the Company’s assets. They would also be in a position to prevent or cause a change in control of the Company.

156. Additionally, the 2016 Proxy states the following under the section entitled “Related Person Transactions Since the Beginning of 2015,” in relevant part:

On June 2, 2015, the Company entered into a stock purchase agreement to repurchase shares of our Common Stock from Nelson Peltz, Peter W. May and Edward P. Garden and certain of their family members and affiliates, investment funds managed by Trian Partners, an investment management firm controlled by Messrs. Peltz, May and Garden, and the general partner of certain of those investment funds (together with Messrs. Peltz, May and Garden, certain of their family members and affiliates and Trian Partners, the “Trian Group”), who in the aggregate owned approximately 24.8% of our outstanding shares as of May 29, 2015. Pursuant to the agreement, the Trian Group agreed not to tender or sell any of its shares in the \$639 million modified Dutch auction tender offer the Company commenced on June 3, 2015. Also pursuant to the agreement, the Company

agreed, following completion of the tender offer, to purchase from the Trian Group a pro rata amount of its shares based on the number of shares the Company purchased in the tender offer, at the same price received by stockholders who participated in the tender offer. On July 17, 2015, after completion of the tender offer, the Company repurchased 18.4 million shares of our Common Stock from the Trian Group at the price paid in the tender offer of \$11.45 per share, for an aggregate purchase price of \$210.9 million.

On December 1, 2011, the Company entered into an agreement with Trian Partners and certain of its affiliates, including Nelson Peltz, Peter W. May and Edward P. Garden (collectively, the “Covered Persons”). Pursuant to the agreement, the Board of Directors, including a majority of the independent directors, approved, for purposes of Section 203 of the Delaware General Corporation Law, the Covered Persons becoming the owners of or acquiring an aggregate of up to 32.5% (subject to certain adjustments set forth in the agreement) of the outstanding shares of our Common Stock, such that no such persons would be subject to the restrictions set forth in Section 203 solely as a result of such ownership (such approval, the “Section 203 Approval”). The agreement (other than the provisions relating to the Section 203 Approval and certain miscellaneous provisions) terminated pursuant to its termination provisions on January 15, 2014.

Each of the related person transactions described above was *reviewed and approved by the Audit Committee* in accordance with the terms of its written charter and the RPT Policy.

157. Based on the foregoing, with respect to defendant Levato, Levato has served as the Chairman of the Audit Committee since prior to the beginning of the Relevant Period and, according to the Audit Committee Charter, Levato is required to satisfy the independence requirements pursuant to Section 10A of the Securities Exchange Act of 1934. Additionally, pursuant to the Audit Committee Charter, Levato was responsible for reviewing and approving the foregoing related party transactions involving defendants Peltz and May. Yet, given Levato’s prior employment with the Company, Trian Group, Limited Partnership and Triangle, Levato has longstanding ties with Peltz and May and therefore, he is not and cannot be considered an independent director and should not have been responsible for reviewing and approving the related party transactions. Accordingly, demand upon Levato is futile and must be excused.

158. With respect to defendant Brolick, Brolick has served as a director of the Company since September 2011 and previously served as President and CEO of the Company from September 2011 to January 2016 and as CEO until his retirement from management duties on May 26, 2016. As conceded by the Company in the 2016 Proxy, defendant Brolick is not an independent director due to his insider status. Additionally, as demonstrated above, Brolick has repeatedly failed to make and/or failed to cause the Company to make full and fair disclosure to the public regarding the effectiveness of the Company's data security policies and regarding the scope and effects of the Data Breach. Accordingly, Brolick is incapable of independently exercising his business judgment thus rendering demand futile.

159. With respect to defendant Penegor, Penegor has served as a director of the Company since May 2016 and as CEO of the Company since May 27, 2016. Penegor joined the Company in June 2013 and served as the President and CFO of Wendy's from January 2016 to May 2016, as Executive Vice President, CFO and International from December 2014 to January 2016 and as Senior Vice President and CFO from September 2013 to December 2014. As conceded by the Company in the 2016 Proxy, Penegor is not an independent director due to his insider status.

160. Further, according to the 2015 Proxy, the Company stated that Penegor, "who was promoted from Senior Vice President and Chief Financial Officer to Executive Vice President, Chief Financial Officer and International, took on additional oversight of the Company's International division, *in addition to maintaining his existing responsibilities for Finance, Development and Information Technology.*" Thus, given that Penegor was primarily responsible for overseeing the Company's information technology department, Penegor either knew or should have known that the Company's data security systems were inadequate and

ineffective and had a duty to implement and oversee effective internal controls over the Company's data security policies. This is especially true given the Company's longstanding recognition of the potential adverse material effect that a data security breach could have on the Company's operations. Based on defendant Penegor's utter failure to implement an effective data security program and monitor the Company's compliance with the foregoing, as well as federal, state and local regulations governing data security and privacy (including, as conceded by the Company, compliance with payment card industry rules), Penegor faces a substantial likelihood of liability rendering him incapable of exercising his business judgment and demand futile.

161. With respect to defendant Mathews-Spradlin, Mathews-Spradlin has served as a director of the Company since February 2015. From 1993 until her retirement in 2011, Mathews-Spradlin worked at Microsoft Corporation, where she served as Chief Marketing Officer ("CMO") and Senior Vice President, Central Marketing Group from 2005 to 2011, Corporate Vice President, Marketing from 2001 to 2005, Vice President, Corporate Public Relations from 1999 to 2001 and head of the Corporate Public Relations function from 1993 to 1999. According to the 2016 Proxy, the Company touts that Mathews-Spradlin "possesses extensive experience in global brand management and a *deep understanding of the technology industry* attributable to her background as a senior executive at Microsoft Corporation." Thus, given Mathews-Spradlin's extensive background in technology due to her long tenure at Microsoft, she either knew or should have known that the Company's data security systems were inadequate and ineffective and had a duty to implement and oversee effective internal controls over the Company's data security policies. This is especially true given the Company's longstanding recognition of the potential adverse material effect that a data security breach could

have on the Company's operations. Based on defendant Mathews-Spradlin's utter failure to implement an effective data security program and monitor the Company's compliance with the foregoing, as well as federal, state and local regulations governing data security and privacy (including, as conceded by the Company, compliance with payment card industry rules), Mathews-Spradlin faces a substantial likelihood of liability rendering her incapable of exercising her business judgment and demand futile.

162. Notwithstanding the foregoing affiliations among the Current Director Defendants, the following Current Director Defendants also have longstanding ties to each other based on the fact that they either previously served as officers or directors of certain of the Company's subsidiaries and/or Wendy's International prior to its merger with the Company in September 2008: (i) N. Peltz previously served as the Company's Chairman and CEO and as a director or manager and an officer of certain of the Company's subsidiaries from April 1993 through June 2007; (ii) May served as the President and COO and as a director or manager and an officer of certain of the Company's subsidiaries from April 1993 through June 2007; (iii) Brolick previously worked at Wendy's International for 12 years, last serving as Senior Vice President of New Product Marketing, Research and Strategic Planning; (iv) Hill served as a director of Wendy's International from 1994 until its merger with the Company in September 2008; and (v) Levato served as Executive Vice President and CFO of the Company and certain of its subsidiaries from April 1993 to August 1996. Therefore, given their longstanding deep rooted ties to each other, defendants N. Peltz, May, Brolick, Hill and Levato are incapable of independently considering a demand to bring suit against one another and accordingly, demand is futile.

163. Finally, as stated in the 2016 Proxy, the entire Board was responsible for risk oversight, and the Board's risk oversight function is supported by a Risk Oversight Committee, which is comprised of members of senior management:

Board's Role in Risk Oversight

The Board of Directors provides oversight with respect to the Company's risk assessment and risk management activities, which are designed to identify, prioritize, assess, monitor and mitigate material risks to the Company, including financial, operational, compliance and strategic risks. While the Board has primary responsibility for risk oversight, the Board's standing committees support the Board by regularly addressing various risks in their respective areas of responsibility. The Audit Committee focuses on financial risks, including reviewing with management, the Company's internal auditors and the Company's independent registered public accounting firm the Company's major risk exposures (with particular emphasis on financial risk exposures), the adequacy and effectiveness of the Company's accounting and financial controls and the steps management has taken to monitor and control such exposures, including the Company's risk assessment and risk management policies. The Compensation Committee considers risks presented by the Company's compensation policies and practices for its executive officers and other employees, as discussed below under the caption "Compensation Risk Assessment." The Nominating and Corporate Governance Committee reviews risks related to the Company's corporate governance structure and processes, including director qualifications and independence, stockholder proposals related to governance, succession planning and the effectiveness of our Corporate Governance Guidelines. ***The Board's risk oversight function is also supported by a Risk Oversight Committee composed of members of senior management. The Risk Oversight Committee is exclusively devoted to prioritizing and assessing all categories of enterprise risk, including risks delegated by the Board of Directors to the Board committees, as well as other operational, compliance and strategic risks facing the Company.*** Each of these committees reports directly to the Board.

(Emphasis added).

164. Based on the foregoing, it can be reasonably inferred that the Board had knowledge of the Company's inadequate and data security measures, given that the Company has acknowledged in its annual statements dating back to 2008 of the potential adverse effect that a security breach would have on the Company's operations. Further, given that the majority of the Company's restaurants are franchisee-owned and the Company derives a substantial

portion of its revenue from its franchisees, the Board either was or should have been aware of the DavCo Lawsuit, especially since DavCo is one of the Company's largest franchisees and Wendy's initiated the lawsuit. Therefore, it can be reasonably inferred that a majority of the Current Director Defendants were on notice of the multiple pervasive problems with the Aloha POS system and yet, failed to take action to address and resolve the deficiencies, including taking steps to ensure that the Company's data security measures were compliant with payment card industry standards. The Board's continued failure to act is further evidenced by the fact that the Company is still utilizing the Aloha POS system despite that restaurants that were using the Aloha POS system were also impacted by the Data Breach, as the Company effectively admitted in its reply to DavCo's Amended Counterclaim. This constitutes bad faith and accordingly, a majority of the Current Director Defendants faces a substantial likelihood of liability rendering them incapable of independently exercising their business judgment and demand futile.

165. The Individual Defendants' conduct described herein and summarized above demonstrates a pattern of misconduct that could not have been the product of legitimate business judgment as it was based on intentional, reckless, and disloyal misconduct. Thus, none of the Individual Defendants, who constitute a majority of the current Board of the Company, can claim exculpation from their violations of duty pursuant to the Company's charter (to the extent such a provision exists). As a majority of the Individual Defendants faces a substantial likelihood of liability, they are self-interested in the transactions challenged herein and cannot be presumed to be capable of exercising independent and disinterested judgment about whether to pursue this action on behalf of the shareholders of the Company.

166. Based on the foregoing, the Current Director Defendants face a sufficiently substantial likelihood of liability and accordingly, there is a reasonable doubt as to each

Defendant's disinterestedness in deciding whether pursuing legal action would be in the Company's best interest. Accordingly, demand upon the Current Director Defendants is excused as being futile.

CAUSES OF ACTION

COUNT I

(Against the Individual Defendants for Breach of Fiduciary Duty)

167. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth herein.

168. The Individual Defendants owed and owe Wendy's fiduciary obligations, including the obligations of good faith, fair dealing, loyalty and care. Among other things, the Individual Defendants owed a fiduciary duty to Wendy's to supervise the issuance of its press releases and public filings and ensure that they were truthful, accurate and conformed to federal and state securities law. The Individual Defendants breached their duties of loyalty, care and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures with respect to data security for the Company and its franchisees; (ii) failing to exercise their oversight duties by not monitoring the Company's compliance with federal and state laws, payment card industry regulations and its agreements with payment card processors and networks; (iii) failing to cause the Company to make full and fair disclosure concerning (a) the effectiveness of the Company's policies and procedures with respect to data security, and (b) the scope and impact of the Data Breach, resulting in the commencement of the Financial Institutions Class Action and Consumer Class Action; (iv) permitting the Company to violate the PCI DSS by, among other things, (a) allowing Wendy's to knowingly operate its point-of-sale system on outdated and unsupported software; (b) failing to ensure that the Company installed and maintained an adequate firewall; (c) failing to ensure that payment card data was properly

segmented from the remainder of Wendy's network; (d) failing to implement necessary protocols, such as software image hardening, password protecting programs that captured payment card data and encrypting payment card data at the point-of-sale; and (e) failing to upgrade the Company's systems to utilize EMV technology; (v) consciously disregarding the systemic and pervasive problems with the Aloha POS system; (vi) consciously permitting the Company to maintain an out of date operating system; and (vii) failing to exercise their oversight duties commensurate with the risk, given the recognition by senior management and the Board that a security breach could adversely affect the Company's business and operations, as evidenced by the fact that the Data Breach went undetected for several months and, it was not until after receiving questions from a third-party concerning banking industry sources who discovered a pattern of fraud on cards that were used at various Wendy's locations that the Company publicly acknowledged that it was investigating claims of a possible credit card breach at some locations.

169. By reason of the foregoing, Wendy's was damaged.

COUNT II
(Against the Individual Defendants for Waste of Corporate Assets)

170. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth herein.

171. Defendants breached their fiduciary duties by failing to properly supervise and monitor Wendy's by allowing the Company to engage in an illegal, unethical and improper course of conduct.

172. As a result of the Individual Defendants' illicit course of conduct and breaches of fiduciary duty, Wendy's has wasted valuable corporate assets through payments of compensation to the Individual Defendants because the Company has incurred significant potential liability

for legal costs, penalties, fines, and/or legal fees in connection with the defense of the Individual Defendants' unlawful course of conduct complained of herein.

173. Additionally, the wrongful conduct alleged herein includes the Individual Defendants' failure to implement adequate internal controls to detect and prevent the Data Breach. Under the Individual Defendants' direction, customers' personal information was unlawfully obtained by unauthorized persons. The Company has already incurred substantial costs in connection with the Data Breach, including investigating and attempting to remedy the breach, and expects to incur even more costs.

174. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company.

175. By reason of the foregoing, Wendy's was damaged.

COUNT III
(Against the Individual Defendants for Unjust Enrichment)

176. Plaintiff incorporates by reference and realleges each of the foregoing allegations as though fully set forth herein.

177. Through the wrongful course of conduct and actions complained of herein, the Individual Defendants were unjustly enriched at the expense of, and to the detriment of Wendy's. The wrongful conduct was continuous and resulted in ongoing harm to the Company. The Individual Defendants were unjustly enriched pursuant to receiving compensation and/or director remuneration while breaching their fiduciary duties to the Company, as alleged herein.

178. Plaintiff, as a shareholder of Wendy's, seeks restitution from the Individual Defendants, and seeks an order of this Court disgorging all profits, benefits, and other

compensation obtained by the Individual Defendants, from their wrongful course of conduct and fiduciary breaches.

179. By reason of the foregoing, Wendy's was damaged.

COUNT IV
(Derivatively Against the Individual Defendants for Gross Mismanagement)

180. Plaintiff incorporates by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

181. By their actions alleged herein, the Individual Defendants, either directly or through aiding and abetting, abandoned and abdicated their responsibilities and fiduciary duties with regard to prudently managing the assets and business of Wendy's in a manner consistent with the operations of a publicly held corporation.

182. As a direct and proximate result of the Individual Defendants' gross mismanagement and breaches of duty alleged herein, Wendy's has sustained significant damages.

183. As a result of the misconduct and breaches of duty alleged herein, the Individual Defendants are liable to the Company.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment as follows:

A. Directing Defendants to account to Wendy's for all damages sustained or to be sustained by the Company by reason of the wrongs alleged herein;

B. Directing Wendy's to take all necessary actions to reform its corporate governance and internal procedures to comply with applicable laws and protect the Company and its shareholders from a recurrence of the events described herein, including, but not limited to, a shareholder vote resolution for amendments to Wendy's By-Laws or Articles of

Incorporation and taking such other action as may be necessary to place before shareholders for a vote on corporate governance policies;

C. Awarding to Wendy's restitution from the Defendants and ordering disgorgement of all profits, benefits and other compensation obtained by the Individual Defendants.

D. Awarding Plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees and expenses; and

E. Granting such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury.

December 16, 2016

Respectfully submitted,

OF COUNSEL:

FARQUI & FARUQI, LLP
Stuart J. Guber
101 Greenwood Avenue, Suite 600
Jenkintown, PA 19046
Telephone: 215-277-5770
Facsimile: 215-277-5771

FARUQI & FARUQI, LLP
Nadeem Faruqi
Nina M. Varindani
685 Third Avenue, 26th Floor
New York, NY 10017
Telephone: 212-983-9330
Facsimile: 212-983-9331

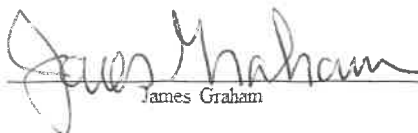
By: /s/Richard S. Wayne
Richard S. Wayne (0022390)
William K. Flynn (0029536)
Thomas P. Glass (0062382)
STRAUSS TROY
The Federal Reserve Building
150 East Fourth Street
Cincinnati, OH 45202-4018
Telephone: (513) 621-2120
Facsimile: (513) 629-9426

Attorneys for Plaintiff

RULE 23.1 VERIFICATION

I, James Graham, am the named Plaintiff to this action. I am a shareholder of The Wendy's Company (the "Company"), and have been at all times throughout the Relevant Period, and approve the filing of this Complaint. I have reviewed the allegations made in this VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT and state that the matters stated therein about which I have personal knowledge are true, and that the other matters stated therein are true and accurate to the best of my knowledge, information and belief, based in part upon the investigation conducted by counsel. Having received a copy of this Complaint, having reviewed it with my counsel, I hereby authorize its filing.

I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 8 day of December, 2016.


James Graham