UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA

BREANDAN COTTER, individually and on behalf of all others similarly situated, Plaintiff, v. CHECKERS DRIVE-IN RESTAURANTS, INC., a Delaware corporation, Defendant.	Case No. **CLASS ACTION COMPLAINT** **INJUNCTIVE RELIEF REQUESTED** JURY TRIAL DEMANDED

Breandan Cotter ("Plaintiff"), by and through his counsel, brings this Class Action Complaint against Defendant Checkers Drive-In Restaurants, Inc. ("Defendant"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to secure and safeguard its customers' credit and debit card numbers and other payment card data ("PCD"), personally identifiable information such as the cardholder's names, payment card number, card verification code, expiration date, and other personal information ("PII") (collectively, "Private Information"), and for failing to provide timely and adequate notice to Plaintiff and other Class members that their Private Information had been stolen and precisely what types of information were stolen.

2. Dating back to September 2016, hackers utilizing malicious software, accessed the point-of-sale ("POS") systems at Defendant's Checkers & Rally's restaurants ("Checkers") throughout the United States and stole copies of Defendant's customers' Private Information (the "Data Breach"). According to Defendant, the hackers maintained operation of the malware in Defendant's POS devices at 102 Checkers locations. Dates vary by location, however, upon information and belief, the malware at issue remained on Defendant's POS devises through April 2019.

3. On May 29, 2019, Defendant confirmed that it had allowed a massive breach of its customers' Private Information to occur, stating that the malware was "designed to collect information stored on the magnetic stripe of payment cards, including cardholder name, payment card number, card verification code and expiration date."[1]

4. Defendant's security protocols were so deficient that the Data Breach continued for years while Defendant failed to even detect it—this despite widespread knowledge of the malicious software (or malware) used to perpetrate the Data Breach, which, upon information and belief, was similar to the malware used to perpetrate the earlier, notorious, and widely reported data breaches affecting retailers Target, Home Depot, Jason's Deli, Arby's, Sonic Drive-In, Pizza Hut, Chipotle, and Wendy's.

5. Defendant has acknowledged the severity of the Data Breach by advising its customers of mitigation efforts such as ordering credit reports and placing fraud alerts and security freezes on their credit reports.

6. Defendant could have prevented this Data Breach. Based upon information and belief, the malicious software used in the Data Breach was similar to the malware strains hackers used in the data breaches at Target, Home Depot, Jason's Deli, Arby's, Sonic Drive-In, Pizza Hut, Chipotle,

[1] https://www.checkers.com/security-issue/ (last visited June 5, 2019).

and Wendy's. While many retailers, banks, and card companies responded to recent breaches, by adopting technology that helps makes transactions more secure, Defendant did not.

7. The susceptibility of POS systems to malware is well-known throughout the restaurant industry. Data security experts have warned companies, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[2]

8. Defendant disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Private Information. On information and belief, Plaintiff's and Class members' Private Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class members' Private Information was compromised and stolen.

9. The Data Breach was the result of Defendant's inadequate approach to data security and protection of Private Information that it collected during the course of its business.

10. As a result of the Data Breach, Plaintiff's and Class members' Private Information has been exposed to criminals for misuse.

11. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for Private Information.

[2] Datacap Systems Inc., *Point of sale security: Retail data breaches at a glance*, https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance# (last visited June 5, 2019)

12. Plaintiff and Class members retain a significant interest in ensuring that their Private Information, which remain in Defendant's possession, are protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for himself and on behalf of similarly situated consumers whose Private Information was stolen.

13. Plaintiff, individually and on behalf of similarly situated consumers, seeks to recover damages, equitable relief, including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries, restitution, disgorgement, reasonable costs and attorney fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 putative class members, and at least some members of the proposed Class have a different citizenship from Defendant.

15. This Court has jurisdiction over Defendant as its headquarters are located in this District.

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

PARTIES

17. Plaintiff Breandan Cotter is a resident and citizen of the state of Georgia. Plaintiff purchased the products and services of Defendant at multiple Checkers location, including the location at 2854 Candler Road, Decatur, Georgia 30034, during the period of the Data Breach.

18. Defendant Checkers Drive-In Restaurants, Inc. is a Delaware corporation with its principal place of business located in Tampa, Florida.

FACTUAL BACKGROUND

A. Checkers' Private Information Collection Practices

19. Defendant operates approximately 860 restaurants in 29 states and the District of Columbia. Defendant expects to expand to 1,200 Checkers restaurants by 2020.

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

21. Through its Privacy Policy,[3] which is available on its website, Defendant advises consumers about the categories of Private Information it collects:

> **INFORMATION WE COLLECT**
>
> Personal Information. The types of information we collect that identify you or relate to you as an individual (**"Personal Information**") may include things such as the following:
>
> 1. Name, *Date of Birth,* mailing address, telephone number, e-mail address, username and password (for account administration), when you supply this information voluntarily
> 2. Device ID, including IP address, which are automatically collected and, while they don't identify you as an individual, do identify a particular computer
> 3. Geolocation (if you are using a mobile application and you consent to this function)
> 4. Financial account information and other payment information (that you submit to us for order processing)

[3] https://www.checkers.com/privacy/ (last visited June 5, 2019).

160.

5. Additional Personal Information you may submit as necessary for the administration of particular promotional events, such as sweepstakes or contests
6. If you are applying for a franchise, date of birth, social security number, contact and employment information

Non-Personal Information. Other types of data will also be collected periodically, such as:

1. Type of browser and operating system, mobile application usage data, and aggregated information such as "click stream" information which means entry and exit points (including referring URLs or domains), traffic statistics, page views, and impressions, all of which are collected automatically
2. Demographic information you choose to submit and which we may combine on an anonymous basis with similar information from other users
3. Information collected through cookies, web beacons, pixel tags and other technologies described in more detail later in the Cookies and Web Beacons section of this Privacy Policy
4. Device Information – Device type, OS and identifier

22. Thus, Defendant stores massive amounts of PII and PCD on its servers and utilizes this information to maximize its profits through predictive marketing and other marketing techniques.

23. Defendant also advises consumers about the use of their Private Information:

USE OR SHARING OF PERSONAL INFORMATION

Except as set forth below, we will not knowingly disclose your Personal Information to anyone outside of Checkers Drive-In Restaurants, Inc., or our affiliated companies or franchisees (collectively "Checkers"):

- **To Perform Services For You**
  We may disclose your Personal Information to third-party service providers to provide us with services such as website hosting, professional services, including information technology services and related infrastructure, customer service, e-mail delivery, auditing and other similar services necessary to the Checkers Online Services and services you request.

- **Corporate Transactions or Events**
  We may disclose your information to a third party in connection with a corporate reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock, including in connection with any bankruptcy or similar proceedings.
- **Compliance with Law**
  We may use or disclose your Personal Information as we deem necessary or appropriate: (1) under applicable law, including laws outside your country of residence; (2) to respond to requests from public and government authorities including public and government authorities outside your country of residence; (3) to comply with subpoenas and other legal processes; (4) to pursue available remedies or limit damages we may sustain; (5) to protect our operations or those of any of our affiliated companies; (6) to protect the rights, privacy, safety or property of Checkers or others ; and (7) to enforce our terms and conditions.
- **Franchise Applications**
  We may disclose the personal information you submit on a franchise application to our business units, agents, parent company, Affiliates and to third parties as part of our consideration of that application and to help conduct our franchise marketing efforts. We require our agents to respect our privacy practices and not use your personal information for purposes other than to carry out our instructions
- **Third Party Marketing**
  If you opt-in to receive marketing communications from third parties, we may, from time to time, share the information you provide to us with a few carefully selected third party marketing partners that we believe offer products or services that may be of interest to you. If you would like us to stop providing your information to our third party marketing partners, you may opt-out by emailing us at MobileCSR@checkers.com or sending a letter to 4300 West Cypress St. Suite 600, Tampa, FL.

24. Defendant further informed consumers of its security safeguards:

SECURITY

We strive to use reasonable safeguards to help prevent loss, misuse and unauthorized access, disclosure or modification of Personal Information provided or collected through the Checkers Online Services. However, no system is perfect or can guarantee that unauthorized access or theft might not occur.

25. On May 29, 2019, Defendant confirmed that it had allowed a massive breach of its customers' Private Information to occur which targeted Private Information stored on the magnetic stripe of payment cards.

26. Plaintiff and Class Members would not have used their credit or debit cards to make purchases at Checkers—indeed, they would not have made purchases at Checkers at all during the period of the Data Breach—had Defendant told them that it lacked adequate computer systems and data security practices to safeguard customers' personally identifiable information from theft.

27. Plaintiff and Class Members suffered actual injury from having their Private Information stolen as a result of the Data Breach.

28. Plaintiff and Class Members suffered actual injury and damages in paying money to and purchasing products and services from Defendant during the Data Breach, expenditures which they would not have made had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' Private Information from theft.

29. Plaintiff and Class Members suffered actual injury in the form of damages to and diminution in the value of their Private Information—a form of intangible property that Plaintiff and Class Members entrusted to Checkers for the purpose of purchasing Defendant products and which was compromised in and as a result of the Data Breach.

30. Plaintiff and Class Members have suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and have concerns for the loss of their privacy.

31. Plaintiff and Class Members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of criminals.

32. Plaintiff and Class Members have a continuing interest in ensuring that their Personal Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

B. Consumers Rely On Defendant's Private Information Security Practices

33. Consumers place value in data privacy and security, and they consider it when making purchasing decisions. Plaintiff would not have made his purchases at Defendant's restaurant had he known that Defendant does not take all necessary precautions to secure its customers' personal and financial data. Defendant failed to disclose its negligent and insufficient data security practices and consumers relied on this omission to make purchases at Defendant's restaurants.

34. Furthermore, when consumers purchase food at a national restaurant chain such as Checkers, they assume that its data security practices and policies are state-of-the-art and that it will use part of the purchase price that consumers pay for such state-of-the-art practices. Consumers thus enter into an implied contract with Defendant that Defendant will adequately secure and protect their Private Information, and will use part of the purchase price of the food to pay for adequate data security measures. In fact, rather than use those moneys to implement adequate data security policies and procedures, Defendant failed to provide reasonable security measures, thereby breaching its implied contract with Plaintiff and Class members.

C. Stolen Private Information Is Valuable to Hackers and Thieves

35. It is well known and the subject of many media reports that Personal Information data is highly coveted and a frequent target of hackers. Personal Information data is often easily taken because it may be less protected and regulated than payment card data.

36. Legitimate organizations and the criminal underground alike recognize the value in Personal Information. Otherwise, they wouldn't pay for it or aggressively seek it. For example, in "one

of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[4]

37. Similarly, in the Target data breach, in addition to PCD data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

38. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id.*

39. Personal Information data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. Unfortunately, and as will be alleged below, despite all of this publicly available knowledge of the continued compromises of Personal Information in the hands of other third parties, such as national restaurant chains, Defendant's approach at maintaining the privacy of Plaintiff's and Class members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

40. Defendant has also recognized the importance of protecting the Private Information exposed in the Data Breach:

> We are significantly dependent upon our computer systems and information technology to properly conduct our business. A significant failure or interruption of service, or a breach in security of our computer systems could cause reduced efficiency in operations, loss of data and business interruptions, and significant capital investment could be required to rectify the problems. In addition, any security breach involving our point of sale or other systems could result in loss of consumer confidence and potential costs associated with consumer fraud.[5]

---

[4] Verizon 2014 PCI Compliance Report, available at https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf ("2014 Verizon Report"), at 54 (last visited June 5, 2019).

[5] United States Securities and Exchange Commission, Form 10-K Report, available at: https://www.sec.gov/Archives/edgar/data/919628/000119312512159019/d275858d10k.htm (last visited June 5, 2019).

41. Despite the recognition of these risks, however, Defendant failed to adequately secure its POS systems, placing the Personal Information of its customers at risk and resulting in the Data Breach.

42. A significant portion of sales at Defendant are made using credit or debit cards. When customers pay using credit or debit cards, Defendant collects Private Information related to those cards including the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. Defendant stores the Private Information in its POS system and transmits this information to a third party for processing and completion of the payment.

43. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information collected, maintained, and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

44. It is well known and the subject of many media reports that Private Information is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches at retailers and restaurant chains, Defendant maintained an insufficient and inadequate system to protect the Private Information of Plaintiff and Class members.

45. Private Information is a valuable commodity because it contains not only payment card numbers but also PII. A "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on multiple underground Internet websites.

46. Private Information is valuable to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, and credit cards.

47. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

48. Defendant was, or should have been, fully aware of the significant volume of daily credit and debit card transactions at Checkers restaurants, and thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

49. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of Private Information in the hands of other third parties, such as retailers and restaurant chains, Defendant's approach to maintaining the privacy and security of Plaintiff's and Class members' Private Information was lackadaisical, cavalier, reckless, or at the very least, negligent.

D. Defendant Failed to Segregate PCD From PII

50. Despite the vulnerabilities of POS systems, available security measures and reasonable businesses practices would have significantly reduced or eliminated the likelihood that hackers could successfully infiltrate business' POS systems.

51. The payment card networks (MasterCard, Visa, Discover, and American Express), data security organizations, state governments, and federal agencies have all implemented various standards and guidance on security measures designed to prevent these types of intrusions into POS systems. However, despite Defendant's understanding of the risk of data theft via malware installed on POS systems, and the widely available resources to prevent intrusion into POS data systems, Defendant failed to adhere to these guidelines and failed to take reasonable and sufficient protective measures to prevent the Data Breach.

52. Unlike PII data, payment card data ("PCD") is heavily regulated. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

53. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data."[6]

54. One PCI DSS requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code.

55. "Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement."[7] However, segregation is recommended because among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data."[8]

56. Illicitly obtained PII and PCD, sometimes aggregated from different data breaches, is sold on the black market, including on websites, as a product at a set price.[9]

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

---

[6] PCI DSS v. 2 at 5 (2010) ("PCI Version 2").

[7] *Id.* at 4.

[8] *See* Verizon Report at 54.

[9] *See, e.g.*, https://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/ (last visited June 5, 2019).

E. The 2019 Data Breach at Checkers Locations

58. Dating back to September 2016, hackers utilizing malicious software, accessed the point-of-sale ("POS") systems at Checkers locations throughout the United States and stole copies of Defendant's customers' Private Information (the "Data Breach"). According to Defendant, the hackers maintained operation of the malware in Defendant's POS devices at 102 Checkers locations. Dates vary by location, however, upon information and belief, the malware at issue remained on Defendant's POS devises through April 2019.

59. Defendant's security protocols were so deficient that the Data Breach continued for years while Defendant failed to even detect it—this despite widespread knowledge of the malicious software (or malware) used to perpetrate the Data Breach, which, upon information and belief, was similar to the malware used to perpetrate the earlier, notorious, and widely reported data breaches affecting retailers Target, Home Depot, Jason's Deli, Arby's, Sonic Drive-In, Pizza Hut, Chipotle, and Wendy's.

60. On May 29, 2019, nearly three years after the malicious software exposing its customers' Private Information, Defendant finally confirmed that it had allowed a massive breach of its customers' Private Information to occur.

F. This Data Breach Will Result In Identity Theft and Identify Fraud

61. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach.

62. The ramifications of Defendant's failure to keep Class members' data secure are severe.

63. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud."[10] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

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

65. In addition, identity thieves may get medical services using consumers' compromised Personal Information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

66. It is incorrect to assume that reimbursing a consumer for fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[11] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

67. Annual monetary losses from identity theft are in the billions of dollars.

---

[10] *See* 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at < https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters (last visited June 5, 2019) (the "2013 Identity Fraud Report").

[11] Victims of Identity Theft, 2012 (Dec. 2013) at 10, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited June 5, 2019).

68. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[12]

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

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

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

G. Plaintiff and Class Members Suffered Damages

71. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class

[12] *See* 2013 Identity Fraud Report.

[13] GAO, Report to Congressional Requesters, at p.33 (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (emphases added) (last visited June 5, 2019).

members' Private Information to protect against reasonably foreseeable threats to the security or integrity of such information.

72. Plaintiff's and Class members' Private Information is private and sensitive in nature and was left inadequately protected by Defendant. Defendant did not obtain Plaintiff's and Class members' consent to disclose their Private Information to any other person as required by applicable law and industry standards.

73. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

74. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit/debit card and Personal Information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet card black market;

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

d. the improper disclosure of their Private Information;

e. loss of privacy;

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

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

h. overpayments to Defendant for food purchased during the Data Breach in that a portion of the price paid by Plaintiff and Class members to Defendant was for the costs of reasonable and adequate safeguards and security measures that would protect customers' Private Information, which Defendant did not implement and, as a result, Plaintiff and Class members did not receive what they paid for and were overcharged by Defendant; and

i. the loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts.

.

75. Plaintiff also purchased food and, thus, enriched Defendant, which he otherwise would not have done had Defendant warned of its lax security practices.

76. Notwithstanding Defendant's wrongful actions and inaction and the resulting Data Breach, Defendant has not offered consumers any credit monitoring and identity theft protection services, instead merely directing customers how to obtain credit reports and implement fraud alerts and security freezes.[14] This response is insufficient because, *inter alia*, it does not address many categories of damages being sought. The cost of adequate and appropriate mitigation, such as coverage or insurance, against the loss position Defendant has placed Plaintiff and Class members in, is ascertainable and is a determination appropriate for the trier of fact.

77. Defendant's response also is insufficient because, as the GAO reported, the Personal Information could be held by criminals and used to commit fraud after any mitigation efforts expire.

[14] https://www.checkers.com/security-issue/ (last visited June 5, 2019).

CLASS ALLEGATIONS

78. Plaintiff seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons residing in the United States who made a credit or debit card purchase at any affected Checkers location during the period of the Data Breach (the "Nationwide Class").

79. Excluded from each of the above Classes are Defendant and any of its affiliates, parents or subsidiaries; all employees of Defendant; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

80. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

81. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

82. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class include potentially millions of customers whose data was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

83. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law

and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Defendant had a duty to protect Private Information;

b. Whether Defendant knew or should have known of the susceptibility of its POS systems to a data breach;

c. Whether Defendant's security measures to protect its POS systems were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and best practices recommended by data security experts;

d. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendant's failure to implement adequate data security measures allowed the breach of its POS data systems to occur;

f. Whether Defendant's conduct constituted unfair or deceptive trade practices;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Private Information of Plaintiff and Class members;

h. Whether Plaintiff and Class members were injured and suffered damages or other losses because of Defendant's failure to reasonably protect its POS systems and data network; and,

i. Whether Plaintiff and Class members are entitled to relief.

84. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a consumer who used his payment cards at affected Checkers locations and had his cards compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class members, and Plaintiff seeks relief consistent with the relief of the Class.

85. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class,

thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

86. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Personal Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

87. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

88. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class member

would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

89. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

90. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its POS systems were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and other best practices recommended by data security experts;

d. Whether Defendant's failure to adequately comply with PCI DSS standards and/or to institute protective measures beyond PCI DSS standards amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the Private Information of Plaintiff and the Class members; and

f. Whether adherence to PCI DSS requirements, FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

91. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to information regarding which of its restaurants were affected by the Data Breach, the time period of the Data Breach, and which customers were potentially affected. Using this information, Class members can be identified and their contact information ascertained for the purpose of providing notice to the Class.

COUNT I
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, Plaintiff and the separate Statewide Class)

92. Plaintiff restates and realleges paragraphs 1 through 91 above as if fully set forth herein.

93. Defendant solicited and invited Plaintiff and Class members to eat at its restaurants and make purchases using their credit or debit cards as a form of payment. Plaintiff and Class members accepted Defendant's offers and used their credit or debit cards to make purchases at Checkers restaurants during the period of the Data Breach.

94. When Plaintiff and Class members purchased and paid for Defendant's services and food products at Checkers using payment cards, they provided their Private Information, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards. In so doing, Plaintiff and Class members on the one hand, and Defendant on the other, entered into mutually agreed-upon implied contracts pursuant to which Plaintiff and Class members agreed that their payment cards were valid and would provide compensation for their purchases, while Defendant agreed that it would use the Private Information of Plaintiff and Class members in its possession for only authorized uses.

95. Implicit in the agreement by Defendant to use the Private Information in its possession for only the agreed-upon uses and no other purpose was the obligation that Defendant would use

reasonable measures to safeguard and protect the Private Information of Plaintiff and Class members in its possession.

96. By accepting payment cards as methods of payment for purchases, Defendant assented to and confirmed its agreement to reasonably safeguard and protect the Private Information of Plaintiff and Class members from unauthorized disclosure or uses and to timely and accurately notify Plaintiff and Class members if their data had been breached and/or compromised.

97. Plaintiff and Class members would not have provided and entrusted their Private Information, including all information contained in the magnetic strips of their credit and debit cards, to Defendant to eat at its restaurants and make purchases in the absence of the implied contract between them and Defendant.

98. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

99. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the Personal Information of Plaintiff and Class members and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

100. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to ensure that the Private Information of Plaintiff and Class members in its possession was used only for the agreed-upon payment for purchases and no other purpose.

101. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their payment information. In exchange, Plaintiff and Class members should have received the goods and services that

were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

102. Defendant knew that Plaintiff and Class members conferred a benefit on Defendant and has accepted or retained that benefit. Defendant profited from the purchases and used the Private Information of Plaintiff and Class members for business purposes.

103. Defendant failed to secure the Private Information of Plaintiff and Class members and, therefore, did not provide full consideration for the benefit the Plaintiff and Class members provided.

104. Defendant acquired the Private Information through inequitable means it failed to disclose the inadequate security practices previously alleged.

105. If Plaintiff and Class members had known that Defendant would employ inadequate security measures to safeguard Private Information, they would not have made purchases at Defendant.

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

107. Plaintiff and Class members were harmed as the result of Defendant's breach of the implied contracts because their Private Information was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Private Information was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. Plaintiff and the Class have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees, and other expenses relating to identity theft losses or protective measures. The Class members are further damaged as their Personal Information remains in the hands of those who obtained it without their consent.

108. This breach of implied contracts was a direct and legal cause of the injuries and damages to Plaintiff and Class members as described above.

109. As a direct and proximate cause of Defendant's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of their Private Information; damages arising from Plaintiff's and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above

COUNT II
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class, or, alternatively,
Plaintiff and the separate Statewide Class)

110. Plaintiff restates and realleges paragraphs 1 through 91 above as if fully set forth herein.

111. Upon accepting and storing the Private Information of Plaintiff and Class members in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and Class

members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

112. Defendant owed a duty of care not to subject Plaintiff and Class members, along with their Private Information, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

113. Defendant owed numerous duties to Plaintiff and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

114. Defendant also breached its duty to Plaintiff and the Class members to adequately protect and safeguard Private Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Private Information of Plaintiff and Class members, misuse the Private Information, and intentionally disclose it to others without consent.

115. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information, the vulnerabilities of POS systems, and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches within the restaurant industry.

116. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

117. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

118. Because Defendant knew that a breach of its systems would damage hundreds of thousands, if not millions, of Defendant customers, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

119. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions to safeguard that information. Moreover, only Defendant had the ability to protect its systems and the Private Information stored on those systems from attack.

120. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure its POS systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

121. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' Private Information and promptly notify them about the Data Breach.

122. Defendant breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class members' Private Information before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' Private Information had been improperly acquired or accessed.

123. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Private Information of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information while it was within Defendant's possession or control.

124. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Private Information to Plaintiff and the Class so that Plaintiff and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

125. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access to their Private Information by waiting to notify Plaintiff and Class members and then by failing to provide Plaintiff and Class members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Plaintiff and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

126. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the Private Information of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class members while it was within Defendant's possession or control.

127. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

128. Upon information and belief, Defendant improperly and inadequately safeguarded Plaintiff's and Class members' Private Information in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect sensitive Private Information as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class members' Private Information.

129. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons

having access to Private Information of Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive Private Information had been compromised.

130. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

131. As a direct and proximate cause of Defendant's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of their Private Information; damages arising from Plaintiff's and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
NEGLIGENCE PER SE
(On behalf of Plaintiff and the Nationwide Class, or, alternatively,
Plaintiff and the separate Statewide Class)

132. Plaintiff restates and realleges paragraphs 1 through 91 above as if fully set forth herein.

133. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices.

134. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[15]

135. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII and PCD, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

136. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

[15] FTC, *Start With Security, supra* note **Error! Bookmark not defined.**.

137. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of a data breach at a restaurant chain as large as Checkers, including, specifically, the immense damages that would result to Plaintiff and Class members.

138. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

139. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

140. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

141. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from

identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

142. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, Plaintiff and the separate Statewide Class)

143. Plaintiff restates and realleges paragraphs 1 through 91 above as if fully set forth herein.

144. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their payment card information. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

145. Defendant knew that Plaintiff and Class members conferred a benefit on Defendant and accepted or retained that benefit. Defendant profited from the purchases and used the Private Information of Plaintiff and Class members for business purposes.

146. Defendant failed to secure the Private Information of Plaintiff and Class members and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

147. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

148. If Plaintiff and Class members knew that Defendant would not secure their Private Information using adequate security, they would not have made purchases at Checkers restaurants using their payment cards.

149. Plaintiff and Class members have no adequate remedy at law.

150. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

151. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement the data management and security measures that are mandated by industry standards.

152. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT V
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class, or, alternatively,
Plaintiff and the separate Statewide Class)

153. Plaintiff restates and realleges paragraphs 1 through 91 above as if fully set forth herein.

154. As previously alleged, Plaintiff and Class members entered into an implied contract that required Defendant to provide adequate security for the Private Information it collected from their payment card transactions. As previously alleged, Defendant owes duties of care to Plaintiff and Class members that require it to adequately secure Private Information.

155. Defendant still possesses Private Information pertaining to Plaintiff and Class members.

156. Defendant has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its POS systems.

157. Accordingly, Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Defendant's lax approach towards data security has become public, the Private Information in its possession is more vulnerable than before.

158. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

159. Plaintiff, therefore, seek a declaration that: (a) Defendant's existing data security measures do not comply with its contractual obligations and duties of care; and (b) in order to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant systems;

e. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

f. conducting regular database scans and security checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendant customers should take to protect themselves.

COUNT VI
VIOLATIONS OF THE OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq*.
(On behalf of Plaintiff and the Nationwide Class**)**

160. Plaintiff restates and realleges paragraphs 1 through 91 above as if fully set forth herein.

161. Plaintiff and Class members are consumers who used their credit or debit cards to purchase food and drink products and services at Defendant's restaurants. These purchases were made primarily for personal, family, or household purposes.

162. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the sale of food and drink products to consumers, including Plaintiff and Class members.

163. Defendant engaged in, and its acts and omissions affect, trade and commerce. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering to sell, and selling food and drink products and services throughout the United States.

164. Defendant, headquartered and operating in Florida, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failure to maintain adequate computer systems and data security practices to safeguard Personal Information;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Personal Information from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiff and Class members;

d. continued acceptance of credit and debit card payments and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of its POS systems that were exploited in the Data Breach; and

e. continued acceptance of credit and debit card payments and storage of other Personal Information after Defendant knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

165. These unfair acts and practices violated duties imposed by laws, including by not limited to the FTCA and Fla. Stat. § 501.171(2).

166. As a direct and proximate result of Defendant's violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Class members suffered actual damages, including but not limited to: 1) paying a premium for Defendant's goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices; 2) the time that Plaintiff and Class Members were deprived of using the accounts affected by this Data Breach. Fla. Stat. § 501.211(2).

167. Also, as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

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

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment PII and PCD by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant systems;

e. Ordering that Defendant purge, delete, and destroy Personal Information not necessary for its provisions of services in a reasonably secure manner;

f. Ordering that Defendant conduct regular database scans and security checks;

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

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

168. Plaintiff brings this action on behalf of himself and Class members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class members, and the public from Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

169. The above practices and acts by Defendant had the tendency to mislead consumers, including Plaintiff and Class members.

170. The above practices and acts by Defendant were unfair and unconscionable.

171. These acts caused substantial injury to Plaintiff and Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

172. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Class members' Personal Information and that the risk of a data breach or theft was high.

173. Defendant's actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

174. Plaintiff and Class members seek relief under the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*, including, but not limited to, actual damages, injunctive relief, and attorney fees and costs, and any other just and proper relief.

COUNT VII
BREACH OF CONFIDENCE
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, Plaintiff and the separate Statewide Class)

175. Plaintiff restates and realleges paragraphs 1 through 91 above as if fully set forth herein.

176. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members provided to Defendant.

177. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

178. Plaintiff and Class Members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

179. Plaintiff and Class Members also provided their respective Private Information to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of information security practices.

180. Defendant voluntarily received in confidence Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

181. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

182. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

183. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

184. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' Private Information had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

185. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy

186. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in his and the Class members' favor and against Defendant as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and his Counsel to represent the Nationwide Class, or in the alternative, the separate Statewide Class;

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

c. For equitable relief compelling that Defendant use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of Private Information compromised;

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

e. For an award of actual damages under Florida's Deceptive and Unfair Trade Practices Act;

f. For an award of attorney's fees costs and litigation expenses, as allowable by law;

g. For prejudgment interest on all amounts awarded; and

h. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 6, 2019.

Attorneys for the Plaintiff and Putative Class

/s/ Patrick A. Barthle
PATRICK A. BARTHLE II
Florida Bar No. 99286

pbarthle@ForThePeople.com
RYAN J. MCGEE
rmcgee@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

JEAN SUTTON MARTIN*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
2018 Eastwood Road Suite 225
Wilmington, NC 28403
Telephone: (813)559-4908
Facsimile: (888) 316-3489
Email: jeanmartin@forthepeople.com

TINA WOLFSON*
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
twolfson@ahdootwolfson.com

*Admission pro hac vice to be submitted

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

BREANDAN COTTER, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff DeKalb County, GA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Morgan & Morgan Complex Litigation Group
201 N. Franklin Street, 7th Floor, Tampa, FL 33602 (813) 223-5505

DEFENDANTS

CHECKERS DRIVE-IN RESTAURANTS, INC., a Delaware corporation,

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 2 U.S. Government Defendant
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance ☐ 120 Marine ☐ 130 Miller Act ☐ 140 Negotiable Instrument ☐ 150 Recovery of Overpayment & Enforcement of Judgment ☐ 151 Medicare Act ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans) ☐ 153 Recovery of Overpayment of Veteran's Benefits ☐ 160 Stockholders' Suits ☐ 190 Other Contract ☐ 195 Contract Product Liability ☐ 196 Franchise	**PERSONAL INJURY** ☐ 310 Airplane ☐ 315 Airplane Product Liability ☐ 320 Assault, Libel & Slander ☐ 330 Federal Employers' Liability ☐ 340 Marine ☐ 345 Marine Product Liability ☐ 350 Motor Vehicle ☐ 355 Motor Vehicle Product Liability ☐ 360 Other Personal Injury ☐ 362 Personal Injury - Medical Malpractice **PERSONAL INJURY** ☐ 365 Personal Injury - Product Liability ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability ☐ 368 Asbestos Personal Injury Product Liability **PERSONAL PROPERTY** ☐ 370 Other Fraud ☐ 371 Truth in Lending ☐ 380 Other Personal Property Damage ☐ 385 Property Damage Product Liability		☐ 625 Drug Related Seizure of Property 21 USC 881 ☐ 690 Other **LABOR** ☐ 710 Fair Labor Standards Act ☐ 720 Labor/Management Relations ☐ 740 Railway Labor Act ☐ 751 Family and Medical Leave Act ☐ 790 Other Labor Litigation ☐ 791 Employee Retirement Income Security Act **IMMIGRATION** ☐ 462 Naturalization Application ☐ 465 Other Immigration Actions	☐ 422 Appeal 28 USC 158 ☐ 423 Withdrawal 28 USC 157 **PROPERTY RIGHTS** ☐ 820 Copyrights ☐ 830 Patent ☐ 835 Patent - Abbreviated New Drug Application ☐ 840 Trademark **SOCIAL SECURITY** ☐ 861 HIA (1395ff) ☐ 862 Black Lung (923) ☐ 863 DIWC/DIWW (405(g)) ☐ 864 SSID Title XVI ☐ 865 RSI (405(g)) **FEDERAL TAX SUITS** ☐ 870 Taxes (U.S. Plaintiff or Defendant) ☐ 871 IRS—Third Party 26 USC 7609	☐ 375 False Claims Act ☐ 376 Qui Tam (31 USC 3729(a)) ☐ 400 State Reapportionment ☐ 410 Antitrust ☐ 430 Banks and Banking ☐ 450 Commerce ☐ 460 Deportation ☐ 470 Racketeer Influenced and Corrupt Organizations ☐ 480 Consumer Credit ☐ 485 Telephone Consumer Protection Act ☐ 490 Cable/Sat TV ☐ 850 Securities/Commodities/ Exchange ☒ 890 Other Statutory Actions ☐ 891 Agricultural Acts ☐ 893 Environmental Matters ☐ 895 Freedom of Information Act ☐ 896 Arbitration ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision ☐ 950 Constitutionality of State Statutes

REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS
☐ 210 Land Condemnation ☐ 220 Foreclosure ☐ 230 Rent Lease & Ejectment ☐ 240 Torts to Land ☐ 245 Tort Product Liability ☐ 290 All Other Real Property	☐ 440 Other Civil Rights ☐ 441 Voting ☐ 442 Employment ☐ 443 Housing/ Accommodations ☐ 445 Amer. w/Disabilities - Employment ☐ 446 Amer. w/Disabilities - Other ☐ 448 Education	**Habeas Corpus:** ☐ 463 Alien Detainee ☐ 510 Motions to Vacate Sentence ☐ 530 General ☐ 535 Death Penalty **Other:** ☐ 540 Mandamus & Other ☐ 550 Civil Rights ☐ 555 Prison Condition ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)

Brief description of cause:
Breach of implied contract, Negligence, Negligence per se, Unjust enrichment, Declaratory Judgment

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 06/06/2019

SIGNATURE OF ATTORNEY OF RECORD /s/ Patrick A. Barthle

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

Print Save As... Reset

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket. **PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

BREANDAN COTTER, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

CHECKERS DRIVE-IN RESTAURANTS, INC., a Delaware corporation,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* CHECKERS DRIVE-IN RESTAURANTS, INC.
c/o Registered Agent
CORPORATION SERVICE COMPANY
1201 HAYS STREET
TALLAHASSEE, FL 32301

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Patrick A. Barthle, Esq.
Morgan & Morgan Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
pbarthle@forthepeople.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset