UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

I TAN TSAO, individually and on behalf of all others similarly situated, Plaintiff, v. Captiva MVP Restaurant Partners, LLC, a Florida limited liability company, doing business as PDQ, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff, I TAN TSAO ("Plaintiff"), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Captiva MVP Restaurant Partners, LLC, doing business as PDQ ("PDQ" or "Defendant"), based upon personal knowledge with respect to Plaintiff's self and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiff brings this class action case against Defendant PDQ for its failures to secure and safeguard customers' credit and debit card numbers and other payment card data ("PCD"), and other personally identifiable information ("PII") which PDQ collected at the time Plaintiff made purchases at a PDQ restaurant, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class members that their PCD and PII (hereinafter, collectively, "Customer Data") had been stolen and precisely what types of information were stolen.

2. On June 22, 2018, PDQ acknowledged that customers who from May 19, 2017, to

April 20, 2018, used payment cards for transactions at PDQ restaurants affected[1] had their Customer Data stolen (the "Data Breach"). PDQ stated that "an unauthorized person (hacker) exploited part of our computer related system and accessed and or acquired personal information from some of our customers."[2]

3. This private Customer Data was compromised due to PDQ's acts and omissions and its failure to properly protect the Customer Data.

4. PDQ could have prevented this Data Breach. Data breaches at other restaurant chains and retail establishments in the last few years have been the result of malware installed on point-of-sale ("POS") systems. While many retailers, restaurant chains, and other companies have responded to recent breaches by adopting technology that helps make transactions more secure, PDQ did not.

5. In addition to PDQ's failure to prevent the Data Breach, PDQ also failed to detect the breach for almost a year.

6. The Data Breach was the inevitable result of PDQ's inadequate approach to data security and the protection of the Customer Data that it collected during the course of its business. The deficiencies in PDQ's data security were so significant that the malware installed by the hackers remained undetected and intact for almost a year.

7. The susceptibility of POS systems to malware is well-known throughout the restaurant industry, as well as the retail industry. In the last five years, practically every major data breach involving retail stores or fast-food restaurant chains has been the result of malware

[1] PDQ represented at "All PDQ locations in operation during some or all of the breach time period, May 19, 2017 – April 20, 2018, were affected. However, the following locations were not affected: Tampa International Airport location at 4100 George J Bean Pkwy, Tampa, FL 33607, Amalie Arena location at 401 Channelside Drive, Tampa, FL 33602, and PNC Arena location at 1400 Edwards Mill Road, Raleigh, NC 27607." See, *Important Information for our Guests on Data Breach* – Notice to Guests from PDQ dated June 22, 2018, available at https://www.eatpdq.com/promos/news/2018/06/22/guestinfo (last visited June 26, 2018).

[2] See *Important Information for our Guests on Data Breach* – Notice to Guests from PDQ dated June 22, 2018, available at https://www.eatpdq.com/promos/news/2018/06/22/guestinfo (last visited June 26, 2018).

placed on POS systems. Accordingly, data security experts have warned companies, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[3] Unfortunately, PDQ's profit-driven decisions to ignore these warning led to the damage upon which this case is based.

8. PDQ disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard Customer Data, failing to take available steps to prevent and stop the Breach from ever happening, and failing to monitor and detect the Breach on a timely basis.

9. As a result of the PDQ's Data Breach, the Customer Data of Plaintiff and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members as a direct result of the Data Breach include:

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

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their debit or credit card accounts because their accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach, including but not limited to foregoing cash back rewards or points;

e. loss of use of and access to their account funds and costs associated with inability

[3] 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 May 24, 2018).

to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Customer Data being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet black market;

h. money paid for products and services purchased at PDQ restaurants during the period of the Data Breach, in that Plaintiff and Class members would not have dined at PDQ had PDQ disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Customer Data;

i. damages to and diminution in value of their Customer Data entrusted to PDQ for the sole purpose of purchasing products and services from PDQ; and

j. the loss of Plaintiff's and Class members' privacy.

10. The injuries to Plaintiff and Class members were directly and proximately caused by PDQ's failure to implement or maintain adequate data security measures for Customer Data.

11. Further, Plaintiff retains a significant interest in ensuring that Plaintiff's Customer Data, which, while stolen, remains in the possession of PDQ, is protected from further breaches, and seeks to remedy the harms he has suffered on behalf of himself and similarly situated consumers whose Customer Data was stolen as a result of the Data Breach.

12. Plaintiff, on behalf of Plaintiff's self and similarly situated consumers, seeks to recover damages, equitable relief, including injunctive relief, to prevent a reoccurrence of the Data Breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

13. 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 PDQ.

14. This Court has jurisdiction over PDQ as its principal place of business is located in 4343 Anchor Plaza Parkway, Suite 1, Tampa, Florida 33634, it operates restaurants serving the public in this District, including the restaurant where Plaintiff made purchases using Plaintiff's payment card, which led to the damages. Through its business operations in this District, PDQ intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because PDQ is headquartered in this District and PDQ operates restaurants within this District and a substantial

part of the events and omissions giving rise to this action occurred in this District, and PDQ has caused harm to Class members residing in this District. Finally, the Tampa Division of this District is proper because PDQ is headquartered in Hillsborough County, Florida.

PARTIES

16. Plaintiff is a citizen of the state of Florida.

17. PDQ, Inc. is a Florida limited liability company, with its principal place of business located in Hillsborough County, Florida.

18. PDQ, a restaurant chain with nearly 70 locations, sells chicken tenders, nuggets, salads, and sandwiches.[4] In 2013, alone, with only 18 restaurants at the time, PDQ grossed $28,500,000 in sales.[5] PDQ restaurants accept payment for goods and services through a point of sale system ("POS system"), through which customers insert credit and debit cards to pay.

STATEMENT OF FACTS

A. Consumer Plaintiff's Transactions

28. On October 8, 2017, Plaintiff purchased food at an affected PDQ restaurant in Pinellas Park, Florida, using his payment card.

29. On October 31, 2017, Plaintiff purchased food again at an affected PDQ restaurant in Pinellas Park, Florida, using his payment card.

30. Plaintiff paid for one of the aforementioned purchases with his Wells Fargo reward Visa, and paid for the other with his Chase reward Visa.

31. Plaintiff made additional purchases at other effected PDQ locations during the breach period with either of the aforementioned payment cards.

[4] *See*, generally, https://www.eatpdq.com/menu (Last visited: 6/28/2018) and https://www.eatpdq.com/locations/find-a-location (last visited 6/28/2018)
[5] http://www.restaurantbusinessonline.com/future-50-2014/pdq

32. The two payment cards Plaintiff used and which were compromised in the Data Breach were connected to a Visa rewards program. When Plaintiff learned of the breach, Plaintiff notified Wells Fargo and Chase. As a result, Plaintiff's cards were canceled. While Plaintiff is awaiting Plaintiff's new rewards credit cards, Plaintiff has to use alternative methods of payment and, thus, has lost the opportunity to accrue those rewards. Additionally, Plaintiff has several accounts set to autopay using these cards that will need to be reset, in addition to the hassle of having to replace cards.

B. PDQ and Its Customer Data Collection Practices

28. In 2017, PDQ officials declined to disclose average store or companywide revenue figures in an interview with Jax Daily Record; however, industry consulting firm Technomic projects the firm grossed about $100 million in sales in 2015, up 250 percent from $28.5 million in 2013.[6]

29. PDQ operates PDQ restaurants, a restaurant chain, which is "a hybrid of fast casual, with fresh and daily made food and sauces and no walk-in freezers, and fast food — but without burgers. The menu focuses on fried and grilled chicken tenders and sandwiches, fries and hand spun milkshakes."[7]

19. PDQ failed to adequately secure its POS systems, placing the purchasing information of its customers at risk and resulting in the Data Breach.

20. When customers pay using credit or debit cards, PDQ collects Customer Data related to those cards including the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. PDQ stores the Customer Data in its POS system and transmits this information to a third party for processing and completion of the

[6] *See*, Mark Gordon, *PDQ on the Rise*, Jax Daily Record (July 5, 2017) https://www.jaxdailyrecord.com/article/pdq-on-the-rise (Last visited: 6/27/2018)
[7] *See Id.*

payment.

21. At all relevant times, PDQ was well-aware, or reasonably should have been aware, that the Customer Data 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.

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

23. Customer Data is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on multiple underground Internet websites. Customer Data 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, or credit cards.

24. Legitimate organizations and the criminal underground alike recognize the value of Consumer Data contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[8]

25. At all relevant times, PDQ knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur

[8] Verizon 2014 PCI Compliance Report, available at: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 10, 2017).

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.

26. PDQ was, or should have been, fully aware of the significant volume of daily credit and debit card transactions at PDQ restaurants, amounting to tens of thousands of daily payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of PDQ's systems.

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

C. PDQ Had Notice of Data Breaches Involving Malware on POS Systems

28. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[9] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[10] The amount of payment card data compromised by data breaches is massive. For example, it is estimated that over 100 million cards were compromised in 2013 and 2014.[11]

29. Most of the massive data breaches occurring within the last several years involved malware placed on POS systems used by merchants. A POS system is an on-site device, much like an electronic cash register, which manages transactions from consumer purchases, both by

[9] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at* https://www.idtheftcenter.org/2016databreaches.html (last visited May 18, 2018).
[10] *Id*.
[11] Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20, 2014), available at: https://origin-www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf (last visited May 17, 2018).

cash and card. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."[12] The payment processor then passes on the payment information to the financial institution that issued the card and takes the other steps needed to complete the transaction.[13]

30. Before transmitting customer data over the merchant's network, POS systems typically, and very briefly, store the data in plain text within the system's memory.[14] The stored information includes "Track 1" and "Track 2" data from the magnetic strip on the payment card, such as the cardholder's first and last name, the expiration date of the card, and the CVV (three number security code on the card).[15] This information is unencrypted on the card and, at least briefly, will be unencrypted in the POS terminal's temporary memory as it processes the data. [16]

31. In order to directly access a POS device, hackers generally follow four steps: infiltration, propagation, exfiltration, and aggregation.[17] In the infiltration phase, an "attacker gains access to the target environment"[18] allowing the hackers to move through a business' computer network, find an entry point into the area that handles consumer payments, and directly access the physical POS machines at in-store locations.[19] Once inside the system the attacker then infects the POS systems with malware, which "collects the desired information . . . and then

[12] *Id*. at 6.
[13] Salva Gomzin, *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions*, 8 (Wiley 2014), *available at:* http://1.droppdf.com/files/IS0md/wiley-hacking-point-of-sale-payment-application-secrets-threats-and-solutions-2014.pdf (last visited July 18, 2017).
[14] *Id*. at 39.
[15] *Id*. at 43-50.
[16] Symantec, *supra* note 13, at 5.
[17] *Point of Sale Systems and Security: Executive Summary*, SANS Institute, 4 (Oct. 2014), available at: https://www.sans.org/reading-room/whitepapers/analyst/point-salesystems-security-executive-summary-35622 (last visited July 18, 2017).
[18] *Id*.
[19] Symantec, *supra* note 11, at 8.

exfiltrates the data to another system" called the "aggregation point."[20]

32. A 2016 report by Verizon confirmed the vast majority of successful breaches leverage legitimate credentials to gain access to the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to capture payment card data.[21]

33. Intruders with access to unencrypted Track 1 and Track 2 payment card data can physically replicate the card or use it online. Unsurprisingly, theft of payment card information via POS systems is now "one of the biggest sources of stolen payment cards."[22] For example, in 2013, hackers infiltrated Target, Inc.'s POS system, stealing information from an estimated 40 million payment cards in the United States. In 2014, over 7,500 self-checkout POS terminals at Home Depots throughout the United States were hacked, compromising roughly 56 million debit and credit cards.[23]

34. Likewise, POS systems at more than 1,000 Wendy's restaurants were infiltrated with malware, resulting in the theft of payment cards data for approximately six months.[24]

35. Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, PDQ was well aware or should have been aware of the need to safeguard its POS systems.

D. PDQ Failed to Comply with Industry Standards

36. Despite the vulnerabilities of POS systems, available security measures and reasonable businesses practices would have significantly reduced or eliminated the likelihood that

[20] SANS Institute, *supra* note 17, at 4.
[21] Verizon, *2016 Breach Investigations Report*, at 33 *available at* https://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (hereafter "2016 Verizon Report"), at 54 (last visited May 18, 2018).
[22] Symantec, *supra* note 11, at 3.
[23] Brett Hawkins, *Case Study: The Home Depot Data Breach,* 7 (SANS Institute, Jan. 2015), available at: https://www.sans.org/reading-room/whitepapers/casestudies/casestudy-home-depot-data-breach-36367 (last visited May 18, 2018).
[24] Krebs on Security, *1,025 Wendy's Locations Hit in Card Breach* (July 8, 2016), https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/ (last visited May 18, 2018).

hackers could successfully infiltrate business' POS systems.

37. 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 PDQ'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, PDQ failed to adhere to these guidelines and failed to take reasonable and sufficient protective measures to prevent the Data Breach.

38. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, four years ago, Symantec recommended "point to point encryption" implemented through secure card readers, which encrypt credit card information in the POS system, preventing malware that extracts card information through the POS memory while it processes the transaction.[25] Moreover, Symantec emphasized the importance of adopting EMV chip technology. Datacap Systems, a developer of POS systems, recommended similar preventative measures.[26]

39. The major payment card industry brands set forth specific security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

40. 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

[25] Symantec, *supra* note 11, at 6.
[26] *See* Datacap Systems, *supra* note 3.

information in a secure environment.[27]

41. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[28] PCI DSS sets the minimum level of what must be done, not the maximum.

42. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, impose the following mandates on PDQ: [29]

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

43. Among other things, PCI DSS required PDQ to properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

44. PCI DSS also required PDQ to not store "the full contents of…the magnetic stripe

[27] *Payment Card Industry Data Security Standard* v3.2, at 5 (April 2016) available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited July 21, 2017).
[28] *Id*.
[29] *Id*.

located on the back of a card" or "the card verification code or value" after authorization.[30]

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

E. PDQ Failed to Comply With FTC Requirements

46. Federal and State governments have likewise 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. According to the FTC, the need for data security should be factored into all business decision-making.[31]

47. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[32] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all

[30] *Id*. at 38 (PCI DSS 3.2.1 and 3.2.2).
[31] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 18, 2018).
[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 18, 2018).

incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

48. 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.[33]

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

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

51. In this case, PDQ was at all times fully aware of its obligation to protect the financial data of PDQ's customers because of its participation in payment card processing networks. PDQ was also aware of the significant repercussions if it failed to do so because PDQ collected payment card data from tens of thousands of customers daily and it knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

[33] FTC, *Start With Security*, *supra* note 31.

52. Despite understanding the consequences of inadequate data security, PDQ failed to comply with PCI DSS requirements and failed to take additional protective measures beyond those required by PCI DSS.

53. Despite understanding the consequences of inadequate data security, PDQ operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take other measures necessary to protect its data network.

F. The PDQ Data Breach

54. PDQ understands the importance of protecting personal information: "PDQ values the relationship we have with our guests and understands the importance of protecting personal information."[34]

55. Further, massive data breaches have plagued the restaurant industry, including national restaurant chains such as Wendy's, Arby's, Chipotle, Popeye's, Noodles & Co., and P.F. Chang's.

56. Based on the data breaches within the restaurant industry, and PDQ's own acknowledgment of the importance of protecting personal information as stated above, PDQ knew or should have known that its systems were at risk for a similar malware data breach.

57. Beginning in May 19, 2017, "[a]n unauthorized person (hacker) exploited part of [PDQ's] computer related system and accessed and or acquired personal information from some of [PDQ's] customers."[35]

[34] *See, Important Information for our Guests on Data Breach*, available at: https://www.eatpdq.com/promos/news/2018/06/22/guestinfo (last visited July 3, 2018)
[35] *Id.*

58. PDQ believes "the attacker gained entry through an outside technology vendor's remote connection tool."[36]

59. The malware allowed the thieves to download and steal copies of PDQ customers' Customer Data.

60. The breach became public on June 22, 2018, through PDQ's announcement. The announcement came almost one year after the Data Breach began, and two months after the Data Breach was detected. PDQ provided only the following information about the breach. The announcement in full[37] was:

> Important Information for our Guests On Data Breach
> JUN 22
>
> **NOTICE TO GUESTS FROM PDQ**
>
> **June 2018**
>
> PDQ values the relationship we have with our guests and understands the importance of protecting personal information.
>
> **WHAT HAPPENED**
>
> We have been the target of a cyber-attack. An unauthorized person (hacker) exploited part of our computer related system and accessed and or acquired personal information from some of our customers. We believe the attacker gained entry through an outside technology vendor's remote connection tool. Based on an investigation, the unauthorized access and or acquisition occurred from May 19, 2017 – April 20, 2018 (breach time period). We learned on June 8, 2018 that credit card information and or some names may have been hacked.
>
> **PDQs AFFECTED**
>
> All PDQ locations in operation during some or all of the breach time period, May 19, 2017 – April 20, 2018, were affected. However, the following locations were not affected: Tampa International Airport location at 4100 George J Bean Pkwy, Tampa, FL 33607, Amalie Arena location at 401 Channelside Drive, Tampa, FL 33602, and PNC Arena location at 1400 Edwards Mill Road, Raleigh, NC 27607.

[36] *Id.*
[37] *Id.*

WHAT INFORMATION WAS INVOLVED

The information accessed and or acquired included some or all of the following: names, credit card numbers, expiration dates, and cardholder verification value. However, it should be noted that the cardholder verification value that may have been accessed or acquired is not the same as the security code printed on the back of certain payment cards (e.g., Discover, MasterCard, and Visa) or printed on the front of other payment cards (e.g., American Express). Based on the nature of the breach, it was not possible to determine the identity or exact number of credit card numbers or names that were accessed or acquired during the breach time period. If you used a credit card for your purchase at a PDQ restaurant during the breach period, then your credit card number, expiration date, cardholder verification value and or name may have been accessed or acquired by a hacker.

WHAT WE ARE DOING

Caring for our customers is a top priority, and once we suspected a possible breach, we acted immediately to address the situation and stop the breach. We initiated an investigation and engaged a cybersecurity firm that conducted a comprehensive forensic review of the attack. We reported the breach to law enforcement and continue to work with authorities and state regulators. We have taken steps to further strengthen the security of our systems to help prevent this type of incident from happening again.

WHAT YOU CAN DO

You should remain vigilant in reviewing your account statements closely, monitoring free credit reports, and report any unauthorized charges to your card issuer immediately. Please see the below sections for additional steps you may take to protect your information.

FOR MORE INFORMATION

If you have questions, please visit www.eatPDQ.com or contact a dedicated PDQ representative at info@eatPDQ.com or (844) 328-1737 on weekdays from 9:00 a.m. to 4:00 p.m. EST.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

> Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
> Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
> TransUnion, PO Box 2000, Chester, PA 19016, www.tuc.com, 1-800-916-8800
>
> Victims of identity theft should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state, whose contact information can be found here. You can obtain information from these sources about fraud alerts and security freezes. You should also contact your local law enforcement agencies and file a police report. Contact for the Federal Trade Commission is as follows:
>
> Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.ftc.gov/idtheft, 1-877-IDTHEFT (438-4338).

61. Plaintiff's and the Class members' Customer Data was compromised due to PDQ's acts and omissions and its failure to properly protect the Customer Data, despite the fact PDQ should have been aware of recent data breaches impacting other national restaurant chains, including the one at P.F. Chang's, Arby's, Chipotle, and Wendy's.

62. In addition to PDQ's failure to prevent the Data Breach, PDQ also failed to detect the breach for nearly a year.

63. Intruders, therefore, had more than 11 months to collect payment card data unabated. During this time, PDQ failed to recognize its systems had been breached and that intruders were stealing data on hundreds of thousands or more of payment cards. Timely action by PDQ likely would have significantly reduced the consequences of the breach. Instead, PDQ took more than eleven (11) months to realize its systems had been breached, and thus contributed to the scale of the breach and the resulting damages.

64. The Data Breach occurred because PDQ failed to implement adequate data security measures to protect its POS networks from the potential danger of a data breach, and failed to implement and maintain reasonable security procedures and practices appropriate to the

nature and scope of the Customer Data compromised in the Data Breach.

65. While many merchants and vendors have responded to recent breaches by adopting technology and security practices that help make transactions and stored data more secure, PDQ has not done so.

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

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

67. Without detailed disclosure to PDQ customers, consumers, including Plaintiff and Class members, have been left exposed, unknowingly and unwittingly, for months to continued misuse and ongoing risk of misuse of their Customer Data without being able to take necessary precautions to prevent imminent harm.

68. The ramifications of PDQ's failure to keep Plaintiff's and Class members' Customer Data secure are severe.

69. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[38] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[39]

70. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[40]

[38] 17 C.F.R § 248.201 (2013).
[39] *Id.*
[40] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

71. Identity thieves can use personal information, such as Plaintiff's and Class members' Customer Data, which PDQ 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.

72. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[41]

73. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[42]

74. 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.[43]

---

[41] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).
[42] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).
[43] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

75. Thus, Plaintiff and Class members now face years of constant surveillance of their Customer Data, 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.

H. Plaintiff and Class Members Suffered Damages

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

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

78. PDQ had the resources to prevent a breach. PDQ made significant expenditures to market its products, but neglected to adequately invest in data security, despite the growing number of POS intrusions and several years of well-publicized data breaches.

79. Had PDQ remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, PDQ would have prevented intrusion into its POS systems and, ultimately, the theft of its customers' Customer

Data.

80. As a direct and proximate result of PDQ'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 which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

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

a. theft of their personal and financial information;

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

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

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

e. the improper disclosure of their Customer Data;

f. loss of privacy;

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

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

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

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

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

l. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data

Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

82. While the Customer Data of Plaintiff and Class members has been stolen, PDQ continues to hold Customer Data of consumers, including Plaintiff and Class members. Particularly, because PDQ has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class members have an undeniable interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

83. Plaintiff seeks relief on behalf of Plaintiff's self and as a representative of all others who are similarly situated. Pursuant to Rule 23(a), (b)(2), (b)(3) and (c)(4), Fed. R. Civ. P., 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 PDQ location during the period of the Data Breach (the "Nationwide Class").

84. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the laws of the individual State of Florida, and on behalf of separate statewide class, defined as follows:

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

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

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

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

88. **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 includes 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.

89. **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 PDQ had a duty to protect Customer Data;

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

c. Whether PDQ'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 PDQ was negligent in failing to implement reasonable and adequate security procedures and practices;

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

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

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

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

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

90. **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 Plaintiff's payment cards at an affected PDQ location and had Plaintiff's card 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.

91. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Consumer Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and are committed to pursuing this matter against PDQ 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's interests.

92. **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 plaintiffs 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 PDQ, and thus, individual litigation to redress PDQ'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.

93. **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.

94. 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 PDQ failed to timely notify the public of the Breach;

b. Whether PDQ owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Customer Data;

c. Whether PDQ's security measures to protect is 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 PDQ's failure to adequately comply with PCI DSS standards and/or to institute protective measures beyond PCI DSS standards amounted to negligence;

e. Whether PDQ failed to take commercially reasonable steps to safeguard the Customer Data 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.

95. Finally, all members of the proposed Classes are readily ascertainable. PDQ 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, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF CONSUMER PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFF AND THE FLORIDA CLASS)

96. Plaintiff restates and realleges Paragraphs 1 through 95 as if fully set forth herein.

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

98. When Consumer Plaintiff and Class members purchased and paid for PDQ's services and food products at PDQ restaurants using payment cards, they provided their Customer Data, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards. In so doing, Plaintiff and Class members entered into mutually agreed-upon implied contracts with PDQ pursuant to which PDQ agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members if their data had been breached and compromised.

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

100. Plaintiff and Class members fully performed their obligations under the implied contracts with PDQ.

101. PDQ breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the PII and PCD of Plaintiff and Class members and by failing to provide timely and accurate notice to them that their Customer Data was compromised as a result of the Data Breach.

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

COUNT II
NEGLIGENCE
(ON BEHALF OF CONSUMER PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFF AND THE FLORIDA CLASS)

103. Plaintiff restates and realleges Paragraphs 1 through 95 as if fully set forth herein.

104. Upon accepting and storing the Customer Data of Plaintiff and Class members in its computer systems and on its networks, PDQ 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. PDQ knew that the Customer Data was private and confidential and should be protected as private and confidential.

105. PDQ owed a duty of care not to subject Plaintiff and Class members, along with their Customer Data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

106. PDQ 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 Customer Data in its possession;

b. to protect Customer Data 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.

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

108. PDQ knew, or should have known, of the risks inherent in collecting and storing Customer Data, the vulnerabilities of POS systems, and the importance of adequate security. PDQ knew about numerous, well-publicized data breaches within the restaurant industry.

109. PDQ knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Customer Data.

110. PDQ breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Customer Data of Plaintiff and Class members.

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

112. PDQ had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust PDQ with their Customer Data was predicated on the understanding that PDQ would take adequate security precautions. Moreover, only PDQ had the ability to protect its systems and the Customer Data it stored on them from attack.

113. PDQ's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Customer Data. PDQ's misconduct included failing to: (1) secure its point-of-sale systems, despite knowing its 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.

114. PDQ also had independent duties under state and federal laws that required PDQ to reasonably safeguard Plaintiff's and Class members' Customer Data and promptly notify them about the Data Breach.

115. PDQ 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 Customer Data of Plaintiff and Class members;

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' Customer Data both 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' Customer Data had been improperly acquired or accessed.

116. Through PDQ's acts and omissions described in this Complaint, including PDQ's failure to provide adequate security and its failure to protect Customer Data of Plaintiff and Class

members from being foreseeably captured, accessed, disseminated, stolen, and misused, PDQ unlawfully breached its duty to use reasonable care to adequately protect and secure Customer Data of Plaintiff and Class members during the time it was within PDQ's possession or control.

117. The law further imposes an affirmative duty on PDQ to timely disclose the unauthorized access and theft of the Customer Data 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 Customer Data.

118. PDQ breached its duty to notify Plaintiff and Class Members of the unauthorized access 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, PDQ 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.

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

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

121. Upon information and belief, PDQ improperly and inadequately safeguarded Customer Data of Plaintiff and Class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. PDQ's failure to take proper

security measures to protect sensitive Customer Data of Plaintiff and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Customer Data of Plaintiff and Class members.

122. PDQ's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: (1) failing to adequately protect the Customer Data; (2) failing to conduct regular security audits; (3) failing to provide adequate and appropriate supervision of persons having access to Customer Data of Plaintiff and Class members; and (4) failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive Customer Data had been compromised.

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

124. As a direct and proximate cause of PDQ'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 the Customer Data of Plaintiff and Class members; 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 CONSUMER PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFF AND THE FLORIDA CLASS)

125. Plaintiff restates and realleges Paragraphs 1 through 95 as if fully set forth herein.

126. 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 PDQ, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form part of the basis of PDQ's duty in this regard.

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

128. PDQ's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

130. 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 its 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.

131. As a direct and proximate result of PDQ's negligence *per se*, Plaintiff and the Class members have suffered, and continue to suffer, injuries damages arising from Plaintiff's and the 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.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF CONSUMER PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFF AND THE FLORIDA CLASSES)

132. Plaintiff restates and realleges Paragraphs 1 through 95 as if fully set forth here.

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

134. PDQ knew that Plaintiff and Class members conferred a benefit on PDQ and accepted and has accepted or retained that benefit. PDQ profited from the purchases and used the Customer Data of Plaintiff and Class members for business purposes.

135. PDQ failed to secure the Customer Data of Plaintiff and Class members and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

136. PDQ acquired the Customer Data through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

137. If Plaintiff and Class members knew that PDQ would not secure their Customer Data using adequate security, they would not have made purchases at PDQ restaurants.

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

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

140. PDQ 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, PDQ should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT V
DECLARATORY JUDGMENT
(ON BEHALF OF CONSUMER PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFF AND THE FLORIDA CLASSES)

141. Plaintiff restates and realleges Paragraphs 1 through 95 as if fully set forth here.

142. As previously alleged, Plaintiff and Class members entered into an implied contract that required PDQ to provide adequate security for the Customer Data it collected from their payment card transactions. As previously alleged, PDQ owes duties of care to Plaintiff and

Class members that require it to adequately secure Customer Data.

143. PDQ still possesses Customer Data pertaining to Plaintiff and Class members.

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

145. Accordingly, PDQ has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that PDQ's lax approach towards data security has become public, the Customer Data in its possession is more vulnerable than previously.

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

147. Plaintiff, therefore, seeks a declaration that: (a) PDQ'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, PDQ 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 PDQ's systems on a periodic basis, and ordering PDQ 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 customer data by, among other things, creating firewalls and access controls so that if one area of PDQ is compromised, hackers cannot gain access to other portions of PDQ systems;

e. purging, deleting, and destroying in a reasonable secure manner Customer Data not necessary for its provisions of services;

f. conducting regular database scanning and securing 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 PDQ customers must 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 THE NATIONWIDE OR, ALTERNATIVELY, PLAINTIFF AND THE FLORIDA CLASSES)

148. Plaintiff restates and realleges Paragraphs 1 through 95 as if fully set forth herein.

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

150. PDQ 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 the Class members.

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

152. PDQ, 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 Customer Data;

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

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

d. continued acceptance of credit and debit card payments and storage of other personal information after PDQ knew or should have known of the security vulnerabilities of the 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 PDQ knew or should have known of the Data Breach and before it allegedly remediated the Breach.

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

154. As a direct and proximate result of PDQ's violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and the Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on

cards that were fraudulently obtained through the use of the Customer Data of Plaintiff and Class members; damages arising from 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. 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.

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

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

B. Ordering that PDQ engage third-party security auditors and internal personnel to

run automated security monitoring;

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

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

E. Ordering that PDQ purge, delete, and destroy in a reasonable secure manner Customer Data not necessary for its provisions of services;

F. Ordering that PDQ conduct regular database scanning and securing checks;

G. Ordering that PDQ 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 PDQ 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 PDQ customers must take to protect themselves.

156. Plaintiff brings this action on behalf of himself and the 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 and the Class members and the public from PDQ's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. PDQ's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

157. The above unfair and deceptive practices and acts by PDQ were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the

Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

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

159. PDQ'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.

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

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request the Court enter judgment in his and the Class members' favor and against PDQ 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 Florida Class;

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

c. For equitable relief compelling PDQ to 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 Customer Data compromised;

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

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

f. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

This Tuesday, July 03, 2018.

/s/ John A. Yanchunis
JOHN A. YANCHUNIS
Florida Bar No. 324681
jyanchunis@ForThePeople.com
RYAN J. McGEE
Florida Bar No. 064957
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*
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road, Suite 225
Wilmington, North Carolina 28403
Tel: (910) 292-6676
jean@jsmlawoffice.com

James J. Rosemergy*
CAREY, DANIS & LOWE
8235 Forsyth, Suite 1100

St. Louis, MO 63105
Tele: 314-725-7700
Direct: 314-678-1064
Fax: 314-721-0905
jrosemergy@careydanis.com

Francis J. "Casey" Flynn, Jr.*
LAW OFFICE OF FRANCIS J. FLYNN, JR.
6220 W. Third Street, Suite 115
Los Angeles, California 90036
Tele: 314-662-2836
Email: Casey@LawOfficeFlynn.com

**Pro Hac Vice to be submitted*

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS

JS 44 (Rev. 06/17)

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

I Tan Tsao

(b) County of Residence of First Listed Plaintiff Pinellas County
(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

Captiva MVP Restaurant Partners, LLC , a Florida limited liability company, d/b/a PDQ

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
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ❒ 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	PERSONAL INJURY	PERSONAL INJURY	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		❒ 820 Copyrights	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	❒ 830 Patent	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	❒ 710 Fair Labor Standards Act	❒ 835 Patent - Abbreviated New Drug Application	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 720 Labor/Management Relations	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	❒ 380 Other Personal Property Damage	❒ 740 Railway Labor Act	SOCIAL SECURITY	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 751 Family and Medical Leave Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit
❒ 190 Other Contract	❒ 360 Other Personal Injury		❒ 790 Other Labor Litigation	❒ 862 Black Lung (923)	❒ 490 Cable/Sat TV
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 791 Employee Retirement Income Security Act	❒ 863 DIWC/DIWW (405(g))	❒ 850 Securities/Commodities/ Exchange
❒ 196 Franchise				❒ 864 SSID Title XVI	☒ 890 Other Statutory Actions
				❒ 865 RSI (405(g))	❒ 891 Agricultural Acts
					❒ 893 Environmental Matters
					❒ 895 Freedom of Information Act
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	❒ 896 Arbitration
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	Habeas Corpus:	❒ 462 Naturalization Application	❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee	❒ 465 Other Immigration Actions	❒ 871 IRS—Third Party 26 USC 7609	❒ 950 Constitutionality of State Statutes
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty			
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	Other:			
	❒ 448 Education	❒ 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)***:
Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2)

Brief description of cause:
Negligence, Negligence Per Se, Unjust Enrichment and FDUTPA

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 07/03/2018

SIGNATURE OF ATTORNEY OF RECORD /s/ John A. Yanchunis

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. When the petition for removal is granted, check this box.
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.