IN THE CIRCUIT COURT OF THE NINTH JUDICIAL CIRCUIT IN AND FOR ORANGE COUNTY, FLORIDA

CASE NO.: _____

SAUL HYMES, ILANA HARWAYNE-GIDANSKY, EDGAR FIERRO, and JOAN LEWIS, individually and on behalf of all others similarly situated, Plaintiffs, v. EARL ENTERPRISES HOLDINGS, INC. Defendant.	**CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Saul Hymes ("Hymes"), Ilana Harwayne-Gidansky ("Harwayne-Gidansky"), Edgar Fierro ("Fierro"), and Joan Lewis ("Lewis") (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals, allege upon personal knowledge of the facts respectively pertaining to their own actions, and upon information and belief as to all other matters, by and through their undersigned counsel, hereby bring this Class Action Complaint against defendant Earl Enterprises Holdings, Inc. ("Earl Enterprises" or "Defendant").

NATURE OF ACTION

1. Plaintiffs assert this class action against Defendant Earl Enterprises for its failure to exercise reasonable care in securing and safeguarding its customers' sensitive personal information ("SPI"), including the names, payment card numbers, payment card expiration dates, and payment card security codes.

2. On March 29, 2019, Defendant announced that it had "become aware of a data security incident potentially affecting payment card information of a limited number of guests that dined at certain of Earl Enterprises' restaurants."[1] Defendant included a list of approximately 100 affected restaurants (largely its chain Buca di Beppo, but also other restaurants including Planet Hollywood and Earl of Sandwich) and stated that the breach involved transactions at restaurants between May 23, 2018, through March 18, 2019 (the "Data Breach").[2]

3. In fact, the breach was much more serious than implied by Earl Enterprises' own press release. Highly respected security blogger Brian Krebs noted that approximately 2.15 million payment card numbers belonging to customers who had patronized Defendant's restaurants were *actively for sale on the dark web* through a site called "Joker's Stash" beginning as early as February 20, 2019 (the "Krebs Report").

4. Defendant 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 data breaches by adopting technology that helps make transactions more secure, Defendant did not.

5. In addition to Defendant's failure to prevent the Data Breach, Defendant also failed to detect the breach for approximately ten months.

6. The Data Breach was the result of Defendant's inadequate approach to data security and protection of SPI that it collected during the course of its business. The deficiencies in

---

[1] http://www.earlenterprise.com/incident/, last accessed March 31, 2019.

[2] *Id.*

Defendant's data security were so significant that the malware installed by hackers remained undetected and intact in Defendant's systems for months.

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 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, Defendant's profit-driven decision to ignore warnings like this led to the damage alleged here.

8. Defendant disregarded the rights of Plaintiffs and the Class 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 SPI, failing to take available steps to prevent and prevent the Data Breach, failing to monitor and timely detect the Data Breach, and failing to provide Plaintiffs and the Class prompt and accurate notice of the Data Breach.

9. As a result of Defendant's Data Breach, Plaintiffs' and Class members' SPI have been exposed to criminals for misuse. The injuries Plaintiffs and the Class suffered as a direct result of the Data Breach include:

i. unauthorized charges on debit and credit card accounts;

ii. theft of personal and financial information;

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

[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#.

iv. damages arising from the inability to use debit or credit card accounts because 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;

v. damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the Data Breach, including, but not limited to, missed bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit;

vi. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, including, but not limited to, lost productivity and opportunity(ies), time taken from the enjoyment of one's life, and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

vii. the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by SPI being exposed for theft and sale on the dark web;

viii. costs of products and services purchased at Defendant's various restaurants during the period of the Data Breach because Plaintiffs and the Class would not have dined at Defendant's various restaurants had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard SPI;

ix. damages to and diminution in value of SPI entrusted to Defendant for the sole purpose of purchasing products and services from Defendant; and

x. the loss of Plaintiffs' and Class members' privacy.

10. The injuries Plaintiffs and the Class suffered were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for SPI.

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

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

PARTIES

13. Plaintiffs Saul Hymes and Ilana Harwayne-Gidansky are citizens of New York and a married couple residing in East Setauket, New York. Collectively, Plaintiffs Saul Hymes and Ilana Harwayne-Gidansky are referred to herein as the "New York Plaintiffs."

14. Plaintiff Edgar Fierro is a citizen of California who resides in Encino, California.

15. Plaintiff Joan Lewis is a citizen of California who resides in Westlake Village in Ventura County, California.

16. Collectively, Plaintiffs Edgar Fierro and Joan Lewis referred to herein as the "California Plaintiffs."

17. Defendant Earl Enterprises Holdings, Inc. is a Florida corporation with its principal place of business at 4700 Millenia Blvd., Suite 400, Orlando, Florida 32839. Defendant operates and maintains a number of restaurants and systems implicated in the Data Breach. Those

restaurants, systems, and related entities include Planet Hollywood International, Inc., Earl of Sandwich (USA), LLC, Buca, LLC, Chicken Guy, LLC, OCS Restaurant Holdings, LLC.

JURISDICTION AND VENUE

18. This is an action for damages and the amount in controversy exceeds this Court's minimum jurisdictional amount ($30,000 exclusive of interest, costs, and attorney's fees).

19. The Court has personal jurisdiction over Earl Enterprises because Earl Enterprises is domiciled in Orange County, Florida.

20. Venue is proper in this Circuit pursuant to section 47.011, Florida Statutes, because Earl Enterprises resides in Orange County, Florida, and because of Florida's common law home venue privilege.

FACTUAL ALLEGATIONS

A. Point-of-Sale Systems

21. The hospitality industry – restaurants, hotels, retail stores, and museums – utilize point-of-sale ("POS") terminals or devices to process customer payments for goods or services. Essentially, a POS terminal is a computerized version of a cash register. POS terminals consist of a computer with specific software programs and have the ability to record and track customer orders, process credit and debit card transactions, connect to other systems in a network, and manage inventory.

22. When a credit or debit card is swiped at a POS terminal, the payment card data (or "PCD") contained on a payment card's magnetic strip is read and briefly stored in the POS terminal's memory while passing through a number of systems and networks before ultimately reaching the retailer's payment processor.

23. PCD is stored in a POS system's memory in plain text and includes "Track 1" and "Track 2" data from the payment card's magnetic strip. Tracks 1 and 2 data includes the cardholder's first and last name, the card's account number and expiration date, and the card's three-digit security code, known as the "CVV." This information, which can be used to clone credit/debit cards and to make purchases online or over the telephone, is unencrypted on the payment card and thus is unencrypted in the POS terminal's memory during processing.

24. POS systems are particularly vulnerable to malware – which is malicious software specifically designed to steal customer payment information. Attacks on POS systems began in 2005. Attackers use network-sniffing malware to intercept credit and debit card data during transmission to payment processors.

25. A malware attack is easy to implement and poses less risk to the attacker in terms of detection and capture as it can be installed remotely.

26. All-in-one POS systems are typically based on operating systems such as Windows Embedded, Windows XP and later versions, in addition to Unix operating systems, such as Linux. Thus, POS systems are highly susceptible to an array of attacks that can result in large data breach incidents.

27. For example, POS systems are vulnerable to "RAM-scraping" malware, which permit attackers to extra data found in memory while the data is processing inside the terminal. Software vulnerabilities are another problem where there is no longer support or patches for POS systems that have older running operating systems such as Windows XP or Windows XP Embedded.

28. POS system attacks happen in stages. Identity thieves typically follow three steps in accessing a POS terminal: infiltration (i.e., gaining access to a network), installation of malware,

and exfiltration. Infiltration is the stage where the attacker gains access to the corporate network by looking for external weaknesses to exploit external-facing systems. For example, attackers can find a periphery device that continues to use a manufacturer's default password or by obtaining a user's credentials through a phishing email sent to a person within an organization.

29. After gaining access to the network, attackers seek to obtain access to the POS system and use an array of strategies to locate the POS systems within the network, such as obtaining a user's credentials via keylogging Trojans, password-hash extraction, cracking, replaying captured login sequences, or through brute force.

30. Once inside, the attacker installs malware or code, which must remain in the breached POS system for a period of time. Unlike data breaches that occur in a database involving hundreds of thousands of records that are quickly accessible, POS malware attackers must wait for transactions to occur and collect data each time a credit or debit card is used.

31. Exfiltration involves transmitting the credit and debit card numbers to the attacker. One method is by using an internal system as a "staging server" that communicates routinely with the POS systems and is able to elude detection. Once enough data is collected, it is then transferred to the hackers

B. Plaintiffs' Transactions

i. The New York Plaintiffs' Transactions

32. On or around February 17, 2019, the New York Plaintiffs purchased food at a Buca di Beppo located at 705 6th Avenue, San Diego, California (the "San Diego Location"), one of the affected locations, using their joint credit card.

33. The New York Plaintiffs continue to monitor their accounts in an effort to detected and prevent any further misuses.

34. Since the announcement, the New York Plaintiffs put a hold on their account, cancelled their credit card, and as of the filing of this complaint, are awaiting the delivery of a new card. Consequently, the New York Plaintiffs have had to forgo using the cancelled credit card, including accumulating credit card rewards points, and must now spend time and effort transferring over automatic payments to the new credit card number after the new card is received.

35. The New York Plaintiffs' joint payment card that was compromised in the Data Breach is connected to a cash-back rewards program. While awaiting a replacement card following the Data Breach and fraudulent charges, the New York Plaintiffs had to use alternative methods of payment and, thus, lost the opportunity to accrue cash-back rewards during that time.

36. Consequently, the New York Plaintiffs lost time dealing with the issues related to the Data Breach in cancelling their credit card, communicating with their financial institution, and in procuring credit freezes to mitigate potential future harm.

37. The New York Plaintiffs would not have used their credit cards to make purchases at Defendant's restaurants during the period of the Data Breach had Defendant disclosed that it lacked adequate computer systems and data security practices to safeguard customers' SPI from theft.

38. The New York Plaintiffs suffered actual injury from having their SPI stolen as a result of the Data Breach.

39. The New York Plaintiffs suffered actual injury and damages in paying money to, and purchasing products from, Defendant's restaurants during the Data Breach, expenditures which they would not have made had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' SPI from theft.

40. The New York Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their SPI—a form of intangible property that the New York Plaintiffs entrusted to Defendant for the purpose of purchasing Defendant's products and which was compromised in and as a result of the Data Breach.

41. The New York Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and have concerns for the loss of their privacy.

42. The New York Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their SPI being placed in the hands of criminals.

43. The New York Plaintiffs have continuing interest in ensuring their SPI, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

ii. Plaintiff Fierro's Transactions

44. Between May 23, 2018 and end of December 2018, Plaintiff Fierro dined and purchased food at a Buca di Beppo located at 17500 Ventura Boulevard, Encino, California (the "Encino Location"), one of the affected locations, on numerous occasions, using his debit card.

45. After dining at the Encino Location, on or around November 2018, Plaintiff Fierro discovered that he had incurred approximately $180.00 of unauthorized charges to his bank account.

46. It took approximately six weeks for Plaintiff Fierro's bank to finally reverse the unauthorized charges, and for Plaintiff Fierro to receive a replacement debit card.

47. Plaintiff Fierro would not have used his debit card to make purchases at Defendant's restaurants had Defendant disclosed that it lacked adequate computer systems and data security practices to safeguard Plaintiff Fierro's personal information from theft.

48. As a result of the data breach, Plaintiff Fierro has suffered damages, including the loss of use of $180.00 for approximately six weeks, among other things.

iii. Plaintiff Lewis' Transactions

49. Between May 23, 2018 and end of December 2018, Plaintiff Lewis dined and purchased food at the Encino Location, on numerous occasions, using her credit card.

50. Between May 23, 2018 and end of December 2018, Plaintiff Lewis also dined and purchased food at a Buca di Beppo located at 205 N. Moorpark Road, Thousand Oaks, California (the "Thousand Oaks Location"), one of the affected locations, on numerous occasions, using the same credit card.

51. After dining at both the Encino and Thousand Oaks Locations, Plaintiff Lewis discovered that she had incurred unauthorized charges on her credit card.

52. Plaintiff Lewis would not have used her credit card to make purchases at Defendant's restaurants had Defendant disclosed that it lacked adequate computer systems and data security practices to safeguard her personal information from theft.

53. Plaintiff Lewis has suffered damages, including the loss of use of her credit card that she uses for virtually all purchases earning points that have value.

54. As a result of the data breach, during the time period of discovering the fraudulent charges and receiving her replacement card, Plaintiff was unable to earn points on her purchases.

55. Further, as a result of the data breach, Plaintiff Lewis has placed fraud alerts with the credit reporting agencies, including the purchase of her credit report to detect and prevent any further misuses.

C. Earl Enterprises' Customer Data Collection Practices

56. Defendant is a for-profit corporation that owns several large restaurant chains, including Buca di Beppo, Planet Hollywood, Earl of Sandwich, as well as smaller restaurants, such as Chicken Guy! and Café Hollywood.

57. As part of the dining process, Defendant's restaurants, like most restaurants, accept payment cards through POS terminals, which accept customer payment card data and process it for payment at the time for which a meal is paid. This data includes the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. Defendant stores the SPI in its POS system and transmits this information to a third party for processing and completion of the payment.

58. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the SPI 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.

59. POS systems and terminals, especially in the hospitality industry, are popular targets for cyberattacks, often involving remote attacks which install malware which can spread through an entire system. The frequency and prevalence of such attacks make it imperative that companies in the hospitality industry (such as Defendant) routinely monitor for malware and cyberattacks and regularly update their software and security procedures.

60. Such malware can go undetected for a long period of time, especially if industry best practices are not routinely used. As *Forbes* Magazine noted, Defendant's breach went

unnoticed for ten months, an "alarming amount of time for point-of-sale malware to go undetected."[4]

61. SPI is a valuable commodity because it contains not only payment card numbers, but also personally identifiable information ("PII"). A "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal, private information on multiple underground Internet websites. SPI is valuable to identity thieves because they can use victims' personal data—including SPI and PII—to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, and credit cards.

62. Legitimate organizations and the criminal underground alike recognize the value of SPI and PII contained in a merchant's data systems; otherwise, the latter 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 SPI and PII] from 38 million users."[5]

63. Professionals tasked with trying to stop fraud and other misuse know that SPI and PII have real monetary value in part because criminals continue their efforts to obtain this data.[6] In other words, if any additional breach of sensitive data did not have incremental value to

---

[4] https://www.forbes.com/sites/leemathews/2019/03/31/planet-hollywood-and-buca-di-beppo-parent-confirms-2-15-million-customer-credit-cards-breached/#d08ef1418c4c, last accessed March 31, 2019.

[5] 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.

[6] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, *CIO Magazine*, http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html, October 2016.

criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. However, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,579 data breaches in 2017, which represents a 44.7 percent increase over the record high figures reported for 2016.[7]

64. The SPI and PII of consumers remains of high value to identity criminals, as evidenced by the prices criminals will pay through black-market sources, or what is often called the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, a complete set of bank account credentials can fetch a thousand dollars or more (depending on the associated credit score or balance available to criminals).[8] Experian reports that a stolen credit or debit card number can sell for $5–110 on the dark web. [9]

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

66. Defendant was, or should have been, fully aware of the significant volume of daily credit and debit card transactions at its 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 Defendant's systems.

---

[7] *2017 Annual Data Breach Year-End Review,* https://www.idtheftcenter.org/2017-data-breaches.

[8] *Here's How Much Thieves Make By Selling Your Personal Data Online, Business Insider,* http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5, May 27, 2015.

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

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

D. Defendant had Notice of Data Breaches Involving Malware on POS Systems

68. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[10] 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.[11] 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.[12]

69. According to a 2018 report by Thales Data Threat Report, Retail Edition, U.S. retailers lead the world in security breaches and have more than doubled, to 50% from 19% since Thales' 2017 report.

70. 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 cash and card. When a payment card is used at a POS terminal, "data contained in the card's magnetic

---

[10] 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.

[11] *Id*.

[12] 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.

stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."[13] The payment processor then passes the payment information on to the financial institution that issued the card and takes the other steps needed to complete the transaction.[14]

71. 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.[15] 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).[16] 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. [17]

72. In order to directly access a POS device, hackers generally follow four steps: infiltration, propagation, exfiltration, and aggregation.[18] In the infiltration phase, an "attacker gains access to the target environment"[19] allowing the hackers to move through a business's computer network, find an entry point into the area that handles consumer payments, and directly access the physical POS machines at in-store locations.[20] Once inside the system the attacker then infects the

---

13 *Id*. at 6.

14 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.

15 *Id*. at 39.

16 *Id*. at 43–50.

17 Symantec, *supra* note 12, at 5.

18 *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.

19 *Id*.

20 Symantec, *supra* note 12, at 8.

POS systems with malware, which "collects the desired information . . . and then exfiltrates the data to another system" called the "aggregation point."[21]

73. 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.[22]

74. 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."[23] 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.[24] 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.[25] The same is true of Brinker, Chipotle, and numerous other retail restaurants.

75. In response to the Target data breach, Connecticut Attorney General George Jepson, who led an investigation of Target, stated "Companies across sectors should be taking their

---

21 SANS Institute, *supra* note 18, at 4.

22 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.

23 Symantec, *supra* note 12, at 3.

24 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.

25 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/.

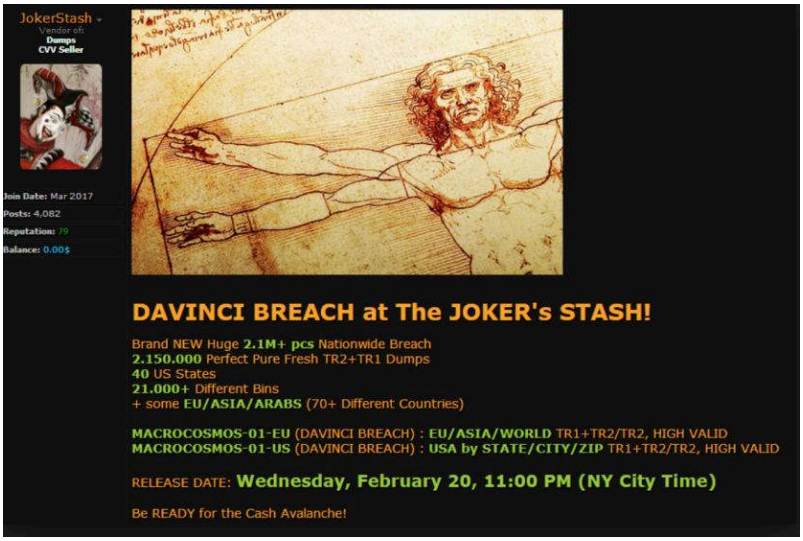
data security policies and procedures seriously. Not doing so potentially exposes sensitive client and customer information to hackers."

76. In 2017, Target announced a multistate settlement to resolve state investigations into the 2013 cyber-attack. Among other things, the settlement requires Target to, among other things: develop, implement and maintain a comprehensive security program; employ an executive or officer responsible for executing the program; hire an independent expert to conduct a security assessment; maintain and support data security software on the company's network, segregate the cardholder data from the rest of the network; and take steps to control network access, including password rotation policies and two-factor identification.

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

E. The Earl Enterprises Data Breach

78. On February 20, 2019, highly respected security blogger Brian Krebs first noticed for sale on a dark web site called "Joker's Stash" a newly-advertised set of 2.15 million payment card numbers for sale.



79. Comparing the zip codes of the locations from which these were stolen to the locations of various chain restaurants, Krebs quickly determined that these likely came from Buca di Beppo, and on February 21, 2019, informed Defendant.

80. Joker's Stash has been described as "the most notorious and well-known underground marketplace for selling stolen credit card dumps."[26]

81. On March 29, 2019, Defendant publicly announced that a security breach had occurred, confirming Krebs' notification.[27] Defendant did not publicly state how many people it believed had been affected, merely stating that it believed a "limited number of guests" were affected.[28]

82. Earl Enterprises also reported that the POS malware attack impacted customers who used credit or debit cards during the period of May 23, 2018 and March 18, 2019 at almost all 67 Buca di Beppo locations in the United States; a handful of Earl of Sandwich locations; Planet Hollywood locations in Las Vegas, New York City and Orlando; Tequila Taqueria in Las Vegas; Chicken Guy! In Disney Springs, Florida; and Mixology in Los Angeles.

83. Further, the limited advice given to customers stated:

> You can carefully review credit and debit card account statements as soon as possible for suspicious charges or activity you do not recognize. As a best practice, we urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card. In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

---

26 https://www.zdnet.com/article/credit-card-details-worth-nearly-3-5-million-put-up-for-sale-on-hacking-forum/, last accessed March 31, 2019.

27 *Id.*

28 https://www.earlenterprise.com/incident/, last accessed March 31, 2019.

> Guests can also review the "Information about Identity Theft Protection" reference guide, included below which describes additional steps that you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.[29]

84. At no point did Defendant offer any concrete assistance or offer to remunerate Plaintiffs or the Class for its negligence.

85. The advertisement on "Joker's Stash" for the payment card numbers specifically stated that it included both Track 1 and Track 2 data.[30] While cloned credit cards can be made from Track 2 data, which is largely limited to account numbers and expiration dates, Track 1 data is more valuable because it also contains names and CVV or CVC codes (the three- or four-digit security codes commonly found on the signature stripe of a credit card).

86. This SPI and PII was compromised due to Defendant's acts and omissions and its failure to properly protect the SPI and PII, despite being aware of recent data breaches impacting other national restaurant chains, including P.F. Chang's, Arby's, Chipotle, Wendy's, Chili's, and other prominent national restaurant chains.

87. In addition to Defendant's failure to prevent the Data Breach, Defendant also failed to detect the breach for nearly ten months.

88. Intruders, therefore, had months to collect SPI and PII unabated. During this time, Defendant failed to recognize its systems had been breached and that intruders were stealing data on millions of payment cards. Timely action by Defendant likely would have significantly reduced the consequences of the breach. Instead, Defendant took more than ten months to realize its

---

[29] *Id.*

[30] https://krebsonsecurity.com/2019/03/a-month-after-2-million-customer-cards-sold-online-buca-di-beppo-parent-admits-breach/, last accessed March 31, 2019.

systems had been breached, and thus contributed to the scale of the Data Breach and the resulting damages to Plaintiffs and Class members.

89. The Data Breach occurred because Defendant 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 SPI and PII compromised in the Data Breach.

90. While many merchants and vendors have responded to recent data breaches by adopting technology and security practices that help make transactions and stored data more secure, Defendant failed to do so.

91. The Data Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting SPI and PII.

92. Additionally, based on a review of state websites that publish company notices of data breaches pursuant to state law (e.g., Cal. Civ. Code § 1798.82(a)), Defendant did not provide written notice to consumers affected by the POS malware attack, although the impacted restaurants collect and maintain contact information for its customers.

93. For example, Buca di Beppo maintains a loyalty program called "Buca E-Club," and collects the names, addresses, and email addresses from its customers and regularly sends marketing emails to such customers. Similarly, Earl of Sandwich also maintains a loyalty program and collects the names, addresses, and email addresses from its customers and regularly sends marketing emails to such customers.

94. Among other things, Defendant failed to provide individual written notice with the following information:

- The type of information that was breached;

- The date or estimated range of the breach;
- The date of the notice;
- Whether notification was delayed due to law enforcement finding that notice would interfere with investigation; and
- A general description of the breach.

F. Defendant Failed to Comply with Industry Standards

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

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

97. Security experts have recommended specific steps that retailers should take to protect their POS systems. For example, a few 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.[31] Moreover, Symantec emphasized the importance of adopting

[31] Symantec, *supra* note 12, at 6.

EMV (Europay, Visa, and Mastercard) chip technology. Datacap Systems, a developer of POS systems, recommended similar preventative measures.[32]

98. Credit card companies announced that retailers must use EMV chip reading machines by October 1, 2015 instead of swiping machines. EMV payment cards contain a microchip that is used to improve payment security and prevent counterfeit card fraud. Consumers insert their cards into the front of a card reader with the metallic square chip facing up instead of swiping cards. Cards with magnetic strips contain unchanging data that can easily be replicated over and over again, unlike the chip cards that create a unique transaction code that cannot be used again. If an attacker steals the chip data from a specific point of sale, card duplication is unavailable because the stolen transaction number created would not be usable again.

99. 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.

100. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.[33]

---

[32] *See* Datacap Systems, *supra* note 3.

[33] *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.

101. 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."[34] PCI DSS sets the minimum level of what must be done, not the maximum.

102. PCI DSS 3.2, the version of the standards in effect at the time of the Data Breach, imposes the following requirements on Defendant: [35]

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

103. Among other things, PCI DSS required Defendant 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.

104. PCI DSS also required Defendant not to store "the full contents of…the magnetic stripe located on the back of a card" or "the card verification code or value" after authorization.[36]

---

34 *Id*.

35 *Id*.

36 *Id*. at 38 (PCI DSS 3.2.1 and 3.2.2).

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

G. Defendant Failed to Comply with Federal and State Requirements

106. 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.

107. There are a number of state and federal laws and requirements and industry standards governing the protection of payment card data.

108. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain personal information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect personal information from unauthorized access. California is one such state and requires that "A business that owns, license, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure." Cal. Civ. Code § 1798.81.5(b). Personal information under these statutes usually is defined to include an individual's first name or initial and last name in combination with a credit or debit card number that is in combination with any required security

code, access code, or password that would permit access to the individual's financial account. See, e.g., Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii).

109. 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.[37]

110. 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.[38] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

111. 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.[39]

---

[37] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[38] 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.

[39] FTC, *Start With Security*, *supra* note 32.

112. 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.

113. Defendant'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.

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

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

116. Despite understanding the consequences of inadequate data security, Defendant 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.

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

117. Without detailed disclosures to Defendant's customers, Plaintiffs and Class members were unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their SPI and PII for up to ten months without being able to take necessary precautions to prevent imminent harm.

i. The New York Plaintiffs' Efforts to Protect their SPI and PII

118. Defendant's Data Breach caused the New York Plaintiffs' credit card to be compromised.

119. New York Plaintiffs have employed extraordinary lengths to protect their identity and maintain their privacy.

120. Prior to the Data Breach, New York Plaintiffs routinely reviewed their financial statements, and the credit card at issue had not been compromised.

121. New York Plaintiffs routinely monitored their credit for unusual activity and had not received any indication that their credit card was breached or otherwise compromised.

122. New York Plaintiffs never transmit unencrypted SPI or PII over the internet or any other unsecured source.

123. New York Plaintiffs store any and all documents containing their SPI and PII in a safe and secure location, and destroy/shred any documents they receive in the mail that contain any of their SPI or PII, or that may contain any information that could otherwise be used to compromise their credit cards, financial accounts, or steal their identities.

ii. Plaintiff Fierro's Efforts to Protect his SPI and PII

124. Defendant's Data Breach caused Plaintiff Fierro's debit card to be compromised.

125. Plaintiff Fierro has employed extraordinary lengths to protect his identity and maintain his privacy.

126. Prior to the Data Breach, Plaintiff Fierro routinely reviewed his financial statements, and the debit card at issue had not been compromised.

127. Plaintiff Fierro routinely monitored his debit card credit for unusual activity and had not received any indication that his debit card was breached or otherwise compromised.

128. Plaintiff Fierro never transmitted unencrypted SPI or PII over the internet or any other unsecured source.

129. Plaintiff Fierro stores any and all documents containing his SPI and PII in a safe and secure location, and destroys and shreds any documents he receives in the mail that contain any of their SPI or PII, or that may contain any information that could otherwise be used to compromise his debit card, financial account, or steal his identity.

iii. Plaintiff Lewis' Efforts to Protect her SPI and PII

130. Defendant's Data Breach caused Plaintiff Lewis to be placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud.

131. Plaintiff Lewis has employed extraordinary lengths to protect her identity and maintain her privacy.

132. Prior to the Data Breach, Plaintiff Lewis routinely reviewed her financial statements, including her credit card statements.

133. Plaintiff Lewis routinely monitored her credit card for unusual activity.

134. Plaintiff Lewis never transmitted unencrypted SPI or PII over the internet or any other unsecured source.

135. Plaintiff Lewis stores any and all documents containing her SPI and PII in a safe and secure location, and destroys and shreds any documents she receive in the mail that contain any of her SPI or PII, or that may contain any information that could otherwise be used to compromise her credit cards, financial accounts, or steal her identity.

iv. The Data Breach Caused Plaintiffs and Class Members to Suffer Injury

136. Thus, given that before the Data Breach, Plaintiffs' credit card had not experienced any prior form of breach or compromise, and they undertook substantial efforts to protect their financial information—including SPI and PII—Defendant's Data Breach is the source of Plaintiffs' damages and injuries described in this Complaint.

137. But for Defendant's Data Breach, Plaintiffs' credit cards would not have been breached or compromised, and their damages would not have occurred.

138. The ramifications of Defendant's failure to keep Plaintiff's and Class members' data secure are severe and far reaching.

139. Consumer victims of data breaches are more likely to become victims of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[40]

140. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[41] 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."[42]

---

40 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

41 17 C.F.R § 248.201 (2013).

42 *Id.*

141. SPI and PII are valuable commodities to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have SPI and PII, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[43]

142. Identity thieves can use SPI and PII, such as that of Plaintiffs and Class members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

143. Analysis of a 2016 survey of 5,028 consumers found "The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[44]

144. As a result of Defendant's delay in notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class members has been driven even higher.

---

[43] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

[44] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new , February 1, 2017.

145. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the six years preceding 2016.[45]

146. 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.[46]

147. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly US $215 per cardholder incurring these charges,[47] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

148. Plaintiffs and the Class now face a real, immediate, and continuing risk of identity theft and fraudulent payment card charges resulting from Defendant's actions and negligence, as well as the expense in forgoing use of cancelled cards and the time and effort expended in changing credit card numbers.

---

45 *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point.

46 Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf.

47 Hadley Malcom, *Consumers Rack Up $14.3 Billion in Gray Charges, Research Study Commissioned For Billguard By Aite Research, Usa Today* (July 25, 2013), available at: https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/.

149. The processes of discovering and dealing with the repercussions of identity theft and fraudulent payments are time consuming and difficult. The Bureau of Justice Statistics reports that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[48]

150. The victims here—Plaintiffs and the Class—are no different, as they are faced with an arduous path to secure their SPI in response to Defendant's negligence. Plaintiffs and the Class must take at least the following steps to attempt to prevent further misuse of their SPI:

a. Review and monitor credit card statements for any unusual or unknown charges;

b. Contact their financial institution to determine if there is any suspicious activity on their accounts;

c. Change their account information;

d. Place a fraud alert on their credit bureau reports;

e. Place a security freeze on their credit bureau reports; and

f. Periodically monitor their credit bureau reports for any unusual activity and check for accuracy.

151. Additionally, there is commonly lag time between when harm occurs and when it is discovered and also between when SPI is stolen and when it is used. According to the U.S. Government Accountability Office, 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.

[48] Erika Harrell and Lynn Langton, *Victims of Identity Theft*, *2012*, (Bureau of Justice Statistics Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

152. There is a very strong probability that those impacted by Defendant's failure to secure their SPI and PII could be at risk of fraud and identity theft for extended periods of time.

153. Thus, Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class are 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, regardless of whether such charges are ultimately reimbursed by banks and credit card companies.

I. Plaintiffs and Class Members Suffered Damages

154. The SPI and PII of Plaintiffs and Class members are private and sensitive in nature and was left inadequately protected by Defendant. Defendant did not obtain Plaintiffs' and Class members' consent to disclose their SPI and PII to any other person as required by applicable law and industry standards.

155. Defendant also failed to notify Plaintiffs and Class Members of the Data Breach, in direct violation of data breach notification laws, such as California Civil Code § 1798.82.

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

157. Defendant had the resources to prevent a breach. Upon information and belief, Defendant 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.

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

159. As a result of Defendant's wrongful actions, inaction, negligent security practices, and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an 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.

160. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' SPI and PII, 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 misused via the sale of Plaintiffs' and Class members' information on the Internet's black market;

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

e. the improper disclosure of their SPI

f. the improper disclosure of their PII;

g. loss of privacy;

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

i. 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;

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

k. 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;

l. 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,

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

161. While Plaintiffs' and Class members' SPI and PII (together and hereinafter referred to as, "Personal Information") have been stolen, Defendant continues to hold SPI and PII of consumers, including Plaintiffs' and Class members' SPI and PII. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and Class members have an undeniable interest in ensuring that their SPI and PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

162. Plaintiffs bring this action on behalf of themselves and as a class action under Florida Rules of Civil Procedure 1.220(a), (b)(2), (b)(3), and (c)(4), seeking damages and equitable relief on behalf of the following nationwide Class for which Plaintiffs seek certification:

> All residents of the United States whose Personal Information was exposed or potentially exposed as a result of the Data Breach Incident (the "Nationwide Class").

163. Additionally, the California Plaintiffs (i.e., Fierro, Lewis, and Zaragoza) bring this action on behalf of themselves and as a class action seeking damages and equitable relief on behalf of the following California Class for which the California Plaintiffs seek certification:

> All persons who reside in California who made a credit or debit card purchase at any affected Earl Enterprises restaurant during the period of the Data Breach (the "California Class").

164. Excluded from the Classes are Defendant; any parent, affiliate, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any of Defendant's officers or directors; or any successor or assign of Defendant. Also excluded are any Judge or court personnel assigned to this case and members of their immediate families.

165. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

166. **Numerosity. Fla. R. Civ. P. 1.220(a)(1).** The Classes are so numerous that joinder of all members is impracticable. While Plaintiffs do not know the exact number of the members of the Classes, Plaintiffs believe the Nationwide Class contains approximately 2.15 million people, and the California Class contains a substantial portion of that 2.15 million people.[49] 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, social media, and/or published notice.

167. **Commonality. Fla. R. Civ. P. 1.220(a)(2), (b)(2).** This action involves common questions of law and fact exist as to all members of the Classes, and predominate over any

[49] For example, Defendant has approximately 77 Buca di Beppo locations across the United States, and 19 of those locations are in California. *See, e.g.*, https://www.bucadibeppo.com/restaurants/. Similarly, Defendant has approximately 34 Earl of Sandwich locations across the United States, and 8 of those locations are in California. *See, e.g.*, https://locations.earlofsandwichusa.com/us.

questions affecting individual members of the Classes. Such questions of law and fact common to the Classes include, but are not limited to:

a. Whether Defendant had a legal duty to implement and maintain reasonable and adequate security procedures and practices for the protection of information it collected and stored on consumers;

b. Whether Defendant had a duty to adequately protect SPI;

c. Whether Defendant had a duty to adequately protect PII;

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

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

f. Whether Defendant engaged in the wrongful conduct alleged herein;

g. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices to protect the information it collected and stored on consumers;

h. Whether Defendant's failure to implement adequate data security measures resulted in or was the proximate cause of the breach of its POS data systems;

i. Whether Defendant's conduct, practices, actions, and/or omissions constituted unfair or deceptive trade practices;

j. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its POS systems, resulting in the loss of the SPI and PII of Plaintiffs and Class members;

k. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and members of the Classes;

l. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and members of the Classes;

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

n. Whether Plaintiffs and Class members are entitled to relief, including equitable relief.

168. **Typicality. Fla. R. Civ. P. 1.220(a)(3).** Plaintiffs' claims are typical of the claims of the members of the Classes. Plaintiffs are consumers who used their payment cards at affected Earl Enterprises locations and had their cards compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class members, and Plaintiffs seek relief consistent with the relief of the Class members.

169. **Adequacy. Fla. R. Civ. P. 1.220(a)(4).** Plaintiffs are adequate representatives of the Classes because Plaintiffs are members of the respective Classes and are committed to pursuing this matter against Defendant to obtain relief for the Classes. Plaintiffs have no conflicts of interest with either Class members. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Classes' interests. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other members of the Classes. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other members of the Classes.

170. **Superiority. Fla. R. Civ. P. 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 Plaintiffs and the Classes are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

171. **Injunctive and Declaratory Relief. Fla. R. Civ. P. 1.220(b)(2).** Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole.

172. **Certification of Specific Issues. Fla. R. Civ. P. 1.220(c)(4).** To the extent a class does not meet the requirements of Rules 1.220(b)(2) or (b)(3), Plaintiffs seek the certification of issues that will drive the litigation toward resolution, as set forth in Paragraphs 167(a)–(n) above.

FIRST CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of all Plaintiffs, the Nationwide Class, and the California Class)

173. Plaintiffs restate and reallege paragraphs 1 through 172 as if fully set forth herein.

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

175. When Plaintiffs and Class members purchased and paid for Defendant's services and food products at Defendant's restaurants using payment cards, they provided their SPI and PII contained on the face of, and embedded in the magnetic strip of, their debit and credit cards. In so doing, Plaintiffs and Class members on the one hand, and Defendant on the other, entered into mutually agreed-upon implied contracts pursuant to which Plaintiffs and Class members agreed that their payment cards were valid and would provide compensation for their purchases, while Defendant agreed that it would use Plaintiffs' and Class members' SPI and PII in its possession for only the agreed-upon payment and no other purpose.

176. Implicit in the agreement to use the SPI and PII in its possession for only the agreed-upon payment and no other purpose was the obligation that Defendant would use reasonable measures to safeguard and protect the SPI and PII of Plaintiffs and Class members in its possession.

177. By accepting payment cards as methods of payment for purchases, Defendant assented to and confirmed its agreement to reasonably safeguard and protect Plaintiffs' and Class members' SPI and PII from unauthorized disclosure or uses and to timely and accurately notify Plaintiffs and Class members if their data had been breached and/or compromised.

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

179. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendant.

180. Defendant breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect Plaintiffs' and Class members' SPI and PII, and by failing to provide timely and accurate notice to them that their SPI and PII was compromised as a result of the Data Breach.

181. Defendant breached the implied contracts it made with Plaintiffs and Class members by failing to ensure that Plaintiffs' and Class members' SPI and PII in its possession was used only for the agreed-upon payment for purchases and no other purpose.

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

183. Defendant knew that Plaintiffs and Class members conferred a benefit on Defendant, and has accepted or retained that benefit. Defendant profited from the purchases and used Plaintiffs' and Class members' SPI and PII for business purposes.

184. Defendant failed to secure Plaintiffs' and Class members' SPI and PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided.

185. Defendant acquired the SPI and PII through inequitable means when it failed to disclose the inadequate security practices previously alleged.

186. If Plaintiffs and Class members had known that Defendant would employ inadequate security measures to safeguard SPI and PII, they would not have made purchases at Defendant's various restaurants.

187. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant on the one hand, and Plaintiffs and Class members on the other, Plaintiffs and Class members sustained actual losses and damages as described in detail above.

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

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

SECOND CLAIM FOR RELIEF
Negligence
(On behalf of all Plaintiffs, the Nationwide Class, and the California Class)

190. Plaintiffs restate and reallege paragraphs 1 through 172 as if fully set forth herein.

191. Defendant solicited and took possession of Plaintiffs' and the Class members' SPI and PII, and Defendant had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure. Defendant also had a duty to timely notify Plaintiffs and the

Class that their SPI and PII had been or may have been stolen. Defendant further had a duty to destroy Plaintiffs' and Class members' SPI and PII within an appropriate amount of time after it was no longer required by Defendant, in order to mitigate the risk of such non-essential SPI and PII being compromised in a data breach.

192. Upon accepting and storing Plaintiffs' and Class members' SPI and PII in its computer systems and on its networks, Defendant undertook and owed a duty of care to Plaintiffs and Class members to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' SPI and PII and to use commercially-reasonable methods to do so. Defendant knew that the SPI and PII was private and confidential, and should be protected as private and confidential.

193. Defendant owed a duty of care not to subject Plaintiffs and Class members, along with their SPI and PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

194. Defendant owed a duty of care to Plaintiffs and Class members to quickly detect a data breach and to timely act on warnings about data breaches.

195. Defendant's duties arose from its relationship to Plaintiffs and Class members and from industry custom.

196. Defendant, through its actions and/or failures to act, unlawfully breached duties to Plaintiffs and Class members by failing to implement standard industry protocols and to exercise reasonable care to secure and keep private the SPI entrusted to it.

197. Defendant, through its actions and/or failures to act, allowed unmonitored and unrestricted access to unsecured SPI and PII.

198. Defendant, through its actions and/or failures to act, failed to provide adequate supervision and oversight of the SPI and PII with which it was entrusted, despite knowing the risk

and foreseeable likelihood of a breach and misuse, which permitted unknown third parties to gather Plaintiffs' and Class members' SPI and PII, misuse that SPI and PII, and intentionally disclose it to unauthorized third parties without consent.

199. Defendant knew, or should have known, the risks inherent in collecting and storing SPI and PII, the vulnerabilities of POS systems, and the importance of adequate security. Defendant was aware of numerous, well-publicized data breaches within the restaurant industry.

200. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' and Class members' SPI and PII.

201. Due to Defendant's knowledge that a breach of its systems would damage millions of its customers, including Plaintiffs and Class members, Defendant had a duty to adequately protect its data systems and the SPI and PII contained thereon.

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

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

204. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class members' SPi and PII, and promptly notify them about the Data Breach.

205. Defendant breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Customer Data;

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 Plaintiffs' and Class members' SPI and PII 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 Plaintiffs' and Class members' SPI and PII had been improperly acquired or accessed.

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

207. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of Plaintiffs' and Class members' SPI and PII, so that Plaintiffs and

Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their SPI and PII.

208. Defendant breached its duty to notify Plaintiffs and Class Members of the unauthorized access to their SPI and PII by waiting to notify Plaintiffs and Class members, and then by failing to provide Plaintiffs and Class members sufficient information regarding the breach.

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

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

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

212. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the SPI and PII; failing

to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class members' SPI and PII; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive SPI and PII had been compromised.

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

214. Defendant's failure to exercise reasonable care in safeguarding SPI and PII by adopting appropriate security measures, including proper encryption storage techniques, was the direct and proximate cause of Plaintiffs' and Class members' SPI and PII being accessed and stolen through the data breach.

215. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' SPI and PII.

216. As a result of Defendant's breach of duties, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of their SPI and PII; damages arising from Plaintiffs' 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.

THIRD CLAIM FOR RELIEF
Negligence *Per Se*
(On behalf of all Plaintiffs, the Nationwide Class, and the California Class)

217. Plaintiffs restate and reallege paragraphs 1 through 172 as if fully set forth herein.

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

219. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect SPI and PII, and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of SPI and PII it obtained and stored, and the foreseeable consequences of a data breach at restaurant chains as large as Defendant's including Planet Hollywood, Buca di Beppo, Earl of Sandwich, and other brands, including, specifically, the immense damages that would result to Plaintiffs and Class members.

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

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

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

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

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

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of all Plaintiffs, the Nationwide Class, and the California Class)

225. Plaintiffs restate and reallege paragraphs 1 through 172 as if fully set forth herein.

226. Plaintiffs and members of the Class conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided and entrusted their SPI and PII to Defendant.

227. In exchange, Plaintiffs and Class members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their SPI and PII with adequate data security.

228. Defendant appreciated, accepted and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and Class Members as described herein; Plaintiffs and Class members conferred a benefit on Defendant and accepted or retained that benefit. Defendant profited from the purchases and used Plaintiffs' and Class members' SPI and PII for business purposes.

229. Defendant failed to secure Plaintiffs' and Class members' SPI and PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided.

230. Defendant acquired the SPI and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

231. If Plaintiffs and Class members knew that Defendant would not secure their SPI and PII using adequate security, they would not have made purchases at Defendant's restaurants using their payment cards.

232. Plaintiffs and Class members have no adequate remedy at law.

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

234. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendant failed to implement the data management and security measures that industry standards mandate.

235. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class members overpaid for security they did not receive.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

FIFTH CLAIM FOR RELIEF
Breach of Confidence
(On behalf of all Plaintiffs, the Nationwide Class, and the California Class)

236. Plaintiffs restate and reallege paragraphs 1 through 172 as if fully set forth herein.

237. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' SPI and PII that Plaintiff and Class Members provided to Defendant.

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

239. Plaintiffs and Class Members provided their respective SPI and PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the SPI and PII to be disseminated to any unauthorized parties.

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

241. Defendant voluntarily received in confidence Plaintiffs' and Class Members' SPI and PII with the understanding that the SPI and PII would not be disclosed or disseminated to the public or any unauthorized third parties.

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

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

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

245. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' SPI and PII. Defendant knew its computer systems and technologies for accepting and securing

Plaintiffs' and Class Members' SPI and PII had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

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

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

SIXTH CLAIM FOR RELIEF
Violation of Florida's Deceptive and Unfair Trade Practices Act
Fla. Stat. § 501.201, *et seq.*
(On behalf of all Plaintiffs and the Nationwide Class)

248. Plaintiffs restate and reallege paragraphs 1 through 172 as if fully set forth herein.

249. Plaintiffs and the Class Members are "consumers." Fla. Stat. § 501.203(7).

250. Plaintiffs and Class Members purchased "things of value" insofar as products and services from Defendant. These purchases were made primarily for personal and family purposes. Fla. Stat. § 501.203(9).

251. Defendant engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale of food and drinks to Plaintiffs and Class members. These food and drinks constitute goods, services, and/or property to consumers, including Plaintiffs and Class Members. Fla. Stat. § 501.203(8).

252. Defendant engaged in, and its acts and omissions affected trade and commerce. Defendant's acts, practices, and omissions were done in the course of Defendant's business of advertising, marketing, offering to sell, and selling goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

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

a. failure to maintain adequate computer systems and data security practices to safeguard SPI and PII;

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

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

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

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

254. This conduct is considered an unfair method of competition, and constitutes unfair and unconscionable acts and practices. Fla. Stat. § 501.204(1).

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

256. As a direct and proximate result of Defendant's violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), Plaintiff and the Class Members suffered actual damages. Fla. Stat. § 501.211(2).

257. Also as a direct result of Defendant's knowing violation of FDUTPA, Plaintiff and Class Members are not only entitled to actual damages, but also declaratory judgment that Defendants' actions and practices alleged herein violate FDUTPA, and injunctive relief, including, but not limited to:

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

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

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

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

v. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner SPI and PII not necessary for their provisions of services;

vi. Ordering that Defendant conduct regular database scanning and securing checks;

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

viii. Ordering Defendant to meaningfully educate their 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 Defendants' customers must take to protect themselves.

Fla. Stat. § 501.211(1).

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

259. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Class members that they could not reasonably avoid; this substantial injury outweighed any

benefits to consumers or to competition.

260. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class members' SPI and PII, and that the risk of a data breach or theft was high.

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

262. Plaintiffs 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.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

SEVENTH CLAIM FOR RELIEF
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq.*
(On behalf of California Plaintiffs and the California Class)

263. California Plaintiffs restate and reallege paragraphs 1 through 12, 14 through 31, 44 through 117, 124 through 161, and 163 through 172, as if fully set forth herein.

264. This claim is brought by California Plaintiffs on behalf of themselves and all California Class members.

265. Defendant's acts and omissions violate the California Customer Records Act, Cal. Civ. Code § 1798.80 et seq.

266. Defendant is a business that owns or licenses personal information about California residents within the meaning of Cal. Civ. Code § 1798.81.5.

267. By failing to implement and maintain appropriate and reasonable security procedures and practices to protect the personal information of California Plaintiffs and the

California Class from unauthorized access and disclosure, Defendant violated Cal. Civ. Code § 1798.81.5.

268. As a result of Defendant's violation of Cal. Civ. Code § 1798.81.5, California Plaintiffs and California Class members have been injured as alleged herein.

269. Accordingly, California Plaintiffs and the California Class have and will incur economic damages relating to time and money spent remedying the breach, including, but not limited to: monitoring their financial accounts to ensure no further fraud is perpetuated; any unauthorized charges are identified and remedied; lack of access to funds while banks and financial institutions issue new cards; and the costs of credit monitoring, purchasing credit reports, and purchasing "freezes" to prevent opening of unauthorized accounts.

270. California Plaintiffs and California Class members are also entitled to injunctive relief and reasonable attorneys' fees and costs pursuant to § 1798.84.

EIGHTH CLAIM FOR RELIEF
Violation of the Security Breach Notification Law
Cal. Civ. Code § 1798.82
(On behalf of California Plaintiffs and the California Class)

271. California Plaintiffs restate and reallege paragraphs 1 through 12, 14 through 31, 44 through 117, 124 through 161, and 163 through 172, as if fully set forth herein.

272. This claim is brought by California Plaintiffs on behalf of themselves and all California Class members.

273. Defendant conducts business in California and owns computerized data that includes the SPI and PII and all information associated with the payment card data of California residents, including California Plaintiffs.

274. California Plaintiffs are California residents and were California residents during the time the Data Breach occurred.

275. Defendant's information security systems were breached in February 2019; however, Defendant did not provide individual or substitute notice informing California Plaintiffs and members of the California Class of the exact nature of the incident, or of how many credit and debit card numbers were affected.

276. By failing to timely disclose to California Plaintiffs and each member of the proposed California Class that their SPI and PII, including their personal information associated with their payment card data was reasonably believed to have been compromised, Defendant violated Cal. Civ. Code § 1798.82.

277. Defendant could have notified California Plaintiffs and the proposed California Class had it implemented and maintained adequate policies and procedures.

278. If Defendant had implemented adequate policies and procedures for the protection of its customers' SPI and PII, it would have discovered the disclosure sooner and could have provided California Plaintiffs and California Class members with notice. Among other things, California Plaintiffs could have taken appropriate measures to protect themselves from identity theft, replace payment cards, and avoid the frustrations associated with remedying fraud.

279. Accordingly, California Plaintiffs and the California Class have and will incur economic damages relating to time and money spent remedying the breach, including, but not limited to: monitoring their financial accounts to ensure no further fraud is perpetuated; any unauthorized charges are identified and remedied; lack of access to funds while banks and financial institutions issue new cards; and the costs of credit monitoring, purchasing credit reports, and purchasing "freezes" to prevent opening of unauthorized accounts.

NINTH CLAIM FOR RELIEF
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On behalf of California Plaintiffs and the California Class)

280. California Plaintiffs restate and reallege paragraphs 1 through 12, 14 through 31, 44 through 117, 124 through 161, and 163 through 172, as if fully set forth herein.

281. This claim is brought by California Plaintiffs on behalf of themselves and all California Class members.

282. Defendant's business practices as complained of herein violate the Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200, et seq. ("UCL").

283. Defendants' practices constitute "unlawful" business practices in violation of the UCL because, among other things, they violate statutory law and the common law, including without limitation Section 5 of the FTC Act, the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*, and the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*

284. Defendant's actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, they are immoral, unethical, oppressive, unconscionable, unscrupulous or substantially injurious to consumers, and/or any utility of such practices is outweighed by the harm caused consumers.

285. Defendants' actions and practices constitute "fraudulent" business practices in violation of the UCL because, among other things, they have a capacity and tendency to deceive members of the public.

286. As a result of Defendants' wrongful business practices, California Plaintiffs and members of the California Class have suffered injury in fact and lost money or property as alleged herein.

287. Defendant's wrongful business practices present an ongoing and continuing threat to the general public.

288. Accordingly, California Plaintiffs and the California Class have and will incur economic damages relating to time and money spent remedying the breach, including, but not limited to: monitoring their financial accounts to ensure no further fraud is perpetuated; any unauthorized charges are identified and remedied; lack of access to funds while banks and financial institutions issue new cards; and the costs of credit monitoring, purchasing credit reports, and purchasing "freezes" to prevent opening of unauthorized accounts.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

TENTH CLAIM FOR RELIEF
Declaratory Judgment
(On behalf of all Plaintiffs, the Nationwide Class, and the California Class)

289. Plaintiffs restate and reallege paragraphs 1 through 172 as if fully set forth herein.

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

291. Defendant still possesses SPI and PII pertaining to Plaintiffs and Class members.

292. Defendant has not announced or otherwise notified Plaintiffs and Class members that their SPI and PII are sufficiently protected or, more importantly, expunged from Defendant's servers so as to prevent any further breaches or compromises.

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

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

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

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

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

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

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

v. purging, deleting, and destroying SPI and PII not necessary for its provisions of services in a reasonably secure manner;

vi. conducting regular database scans and security checks;

vii. 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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class, respectfully seeks from the Court the following relief:

a. Certification of the Class as requested herein;

b. Appointment of Plaintiffs as Class representatives and their undersigned counsel as Class counsel;

c. Award Plaintiffs and members of the proposed Class damages;

d. Award Plaintiffs and members of the proposed Class equitable, injunctive and declaratory relief, including the enjoining of Defendant's insufficient data protection practices at issue herein and Defendant's continuation of its unlawful business practices as alleged herein;

e. An order declaring that Defendant's acts and practices with respect to the safekeeping of SPI and PII are negligent;

f. Award Plaintiffs and members of the proposed Class pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiffs and members of the proposed Class reasonable attorney fees and costs of suit, including expert witness fees; and

h. Award Plaintiffs and members of the proposed Class any further relief the Court deems proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable.

Dated: July 26, 2021

Respectfully submitted,

/s/ John A. Yanchunis

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis
jyanchunis@ForThePeople.com
Ryan J. McGee
rmcgee@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
Matthew M. Guiney (*pro hac vice* forthcoming)
guiney@whafh.com
270 Madison Avenue
New York, New York 10016
Telephone: 212/545-4600
Facsimile: 212/545-4653

WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC
Carl Malmstrom (*pro hac vice* forthcoming)
malmstrom@whafh.com
111 W. Jackson St., Suite 1700
Chicago, IL 60604
Telephone: 312/984-0000
Facsimile: 212/545-4653

WALSH BANKS LAW
Brian M. Walsh (FBN 10968)
brian.walsh@walshbanks.com
105 E. Robinson Street, #303
Orlando, FL 32801

Tel: (407) 259-2426
Fax: (407) 391-3626

LEVI & KORSINSKY LLP
Mark S. Reich (*pro hac vice* forthcoming)
mreich@zlk.com
Courtney E. Maccarone (*pro hac vice* forthcoming)
cmaccarone@zlk.com
55 Broadway, 10th Floor
New York, NY 10006
Tel: (212) 363-7500

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
Gayle M. Blatt (*pro hac vice* forthcoming)
gmb@cglaw.com
110 Laurel Street
San Diego, CA 92101
Tel.: (619) 238-1811
Fax: (619) 544-9232

Attorneys for Plaintiffs and the Putative Class