

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS
URBANA DIVISION

BARBARA IRWIN, on Behalf of Herself and
All Others Similarly Situated,

Plaintiffs,

v.

JIMMY JOHN’S FRANCHISE, LLC,
JIMMY JOHN’S ENTERPRISES, LLC a/k/a
JIMMY JOHN’S LLC,

Defendants.

§ Case No. _____
§
§ CLASS ACTION COMPLAINT
§
§ **JURY TRIAL DEMANDED**
§
§
§
§
§
§
§
§
§

Plaintiff Barbara Irwin, by her attorneys and on behalf of herself and all others similarly situated (the “Class”), bring this action against Defendants Jimmy John’s Franchise, LLC, and Jimmy John’s Enterprises, LLC (“Defendants” or “Jimmy John’s”). Plaintiff alleges the following based upon personal knowledge as to herself and her own acts, and information and belief as to all other matters based upon, inter alia, an investigation conduct by itself and through its attorneys.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Jimmy John’s for failure to secure and safeguard its customers’ personal and financial data, including credit and debit card information, and for failing to expediently inform Plaintiff and the Class that Jimmy John’s had experienced a data breach and that the Plaintiffs’ personal financial information had been acquired by a an unauthorized person.

2. Defendants own, operate and/or control a franchised chain of sandwich restaurants with over 2,000 locations nationwide and/or control the implementation, servicing, and execution of each of the franchised restaurants customer sales transactions systems.

3. Beginning approximately June 16, 2014 unidentified perpetrators accessed and monitored the point-of-sale (POS) systems of no less than 216 locations owned or franchised by Defendants (the “Data Breach”). As a result of the Data Breach, the perpetrators obtained personal and financial information of thousands of individuals, information which includes, but is not limited to, credit and debit card numbers, cardholder names, verification codes, and/or card expiration dates.

4. Although Defendants learned of the breach by at least July 30, 2014, the breach continued throughout August and into September. And, despite its knowledge, Defendants did not any attempt to inform Plaintiff or the Class of the Data Breach until the end of September 2014. Finally on September 24, 2014, the Company issued a public press release acknowledging that its customers’ credit and debit card data were compromised as a result of a remote intrusion into Defendant’s POS. In the press release, Defendants admitted that the Data Breach was ongoing from between June 16, 2014 and September 5, 2014.

5. The security breach, and the failure to promptly discover and block the Data Breach, was the result of Jimmy John’s grossly inadequate information systems and security oversight. These failures enabled the perpetrators to obtain customers’ financial data from Jimmy John’s and subsequently use this information to steal from Jimmy John’s customers’ accounts. Jimmy John’s failures further put the Class members at serious risk of ongoing financial loss and identity theft.

PARTIES

1. Plaintiff Barbara Irwin is a citizen of the State of Arizona residing in Glendale, Arizona.

2. Defendant Jimmy John's Franchise, LLC is a Delaware limited liability company with its principal place of business in Champaign, Illinois that controls, contracts with and/or operates sandwich restaurants and franchises within the state of Arizona.

3. Jimmy John's Enterprises, LLC a/k/a Jimmy John's, LLC is a Delaware principal place of business in Champaign, Illinois that controls, contracts with and/or operates sandwich restaurants and franchises within the state of Arizona. To conduct business in Arizona, Jimmy John's Enterprises maintains a registered office in Phoenix, Arizona and operates in Arizona, Arizona under the registered trade name of Jimmy John's Gourmet Sandwiches.

4. Jimmy John's Franchise, LLC and Jimmy John's Enterprises, LLC is collectively referred to herein as "Jimmy John's" or the "Company."

JURISDICTION AND VENUE

5. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of \$5,000,000 and Plaintiff, and other members of the proposed Class, are citizens of a state different from Defendant.

6. This Court has personal jurisdiction over Jimmy John's because the Company is registered with the Illinois Secretary of State to conduct business in the State of Illinois, has substantial or continuous and systematic contacts through its headquarters located in Champaign, Illinois and maintains stores and employees in the State of Illinois.

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 in that many of the acts and transactions giving rise to this action occurred in this district and because defendant:

- a. is authorized to conduct business in this district and has intentionally availed itself of the laws and markets within this district through the promotion, marketing, distribution and sale of its products in this district;
- b. does substantial business in this district;
- c. maintains its headquarters in this district; and
- c. is subject to personal jurisdiction in this district.

COMMON FACTUAL ALLEGATIONS

8. According to the Company's website, the Company has grown to more than 2,000 locations in 43 states. Of these, 200 have opened per year over the past 3 years and as of 2013, 98% of locations were franchise-owned.

9. When consumers make purchases at the Company's stores using credit or debit cards, the Company collects information related to that card including the card holder name, the account number, expiration date, card verification value (CVV), and PIN for debit cards. The Company stores this information in its point-of-sale system and transmits this information to a third party for completion of the payment. Upon information and belief, the Company also collects and stores customer names, mailing addresses, phone numbers, and email addresses.

10. While the Company's collection of customer information may itself be legal, by collecting and storing such extensive and detailed customer information, the Company creates an obligation for itself to use every means available to it to protect this information from falling into the hands of identity thieves and other criminals.

11. Between approximately June 16, 2014 and through September 5, 2014, unauthorized third parties, commonly referred to as computer hackers, began to monitor and scrape data from at least 216 POS terminals at Defendant's owned or franchised locations. As a result of the intrusion, personal and/or financial information of thousands, if not tens of thousands, of consumers stored by the Company was compromised.

12. According to Defendants, on July 30, 2014, Jimmy John's learned of the security incident affecting its POS system, and purported to begin an investigation into the breach.

13. On July 31, 2014, the first public report of the Company's data breach was made – not by Jimmy John's itself, but by computer security blogger Brian Krebs on his website, KrebsOnSecurity, an online security blog watched by the security industry. In the report, Krebs reported that multiple banks were seeing a pattern of fraud on cards recently used at Jimmy John's locations around the country.

14. The Data Breach continued through at least September 5, 2014.

15. Defendants failed to promptly and adequately notify its customers of the Data Breach. Finally, on September 24, 2014, the Company issued a press release informing customers that “it appears that customers’ credit and debit card data were compromised after an intruder . . . remotely access[ed] the point-of-sale systems at some corporate and franchised locations between June 16, 2014 and September 5, 2014.”

16. The September 24, 2014 Press Release means of notifying the Class of the Data Breach was not only belated but entirely inadequate. Upon information and belief, Defendants’ failed to alert customers of the breach individually through the direct means of communication it has with its customers, including through its large database of customer email addresses or indirect means through its Facebook or Twitter accounts. Although Defendants provided a link to further

information on the breach on its webpage home through a link titled “Data Security Incident,” the location and manner of alert was not conspicuous but instead was buried below the means the website is prominently used (for placing orders), under large scrolling pictures marketing its business, and utilized a font that was the same size and color of that of other links on its homepage (red). Defendants’ failure to provide adequate notice prevented Class members from being able to take action to prevent harm from the Data Breach.

17. The personal and financial information of consumers, including Consumer Plaintiff and Class members, is valuable.

18. The FTC warns consumers to pay particular attention to how they keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. As the FTC notes, “[t]hat’s what thieves use most often to commit fraud or identity theft.”

19. The information stolen from Jimmy John’s, including Plaintiff’s and Class members’ financial and personal information is extremely valuable to thieves. As the FTC recognizes, once identity thieves have personal information, “they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance.”

20. Personal and financial information such as that stolen in Jimmy John’s data breach is highly coveted by and a frequent target of hackers. Legitimate organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use biographical data to perpetuate more and larger thefts.

21. Hackers use the credit card information to create counterfeit credit cards that can be swiped and used to make purchases as if they were real credit cards. Additionally, the thieves could reproduce stolen debit cards and use them to withdraw cash from ATMs.

22. Equally troubling is that Jimmy John's was utilizing a point-of-sale system that did not meet basic security requirements set forth by the PCI Security Standards Council. The Company used software developed by Signature Systems called PDQ POS. PDQ was not approved for new installations after October 28, 2013. Additionally, the Company that performed the security audit on PDQ, defunct firm Chief Security Officers, is the only qualified security assessment firm to have had their certification authority revoked by the PCI Security Standards Council.

23. A number of retailers, banks and card companies have responded to recent security breaches by adopting the use of microchips in U.S. credit and debit cards to make transactions more secure. The Company did not have any such technology in place at any time during the Breach.

24. The Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. The Company grossly failed to comply with security standards and allowed its customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Breach that occurred.

25. Defendant's failure to comply with reasonable security standards provided the Company with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of its own customers – including Class members

here – who have been subject to the Breach or otherwise have had their financial information placed at serious and ongoing risk.

26. The Company allowed widespread and systematic theft of its customers' financial information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information.

PLAINTIFF'S FACTUAL ALLEGATIONS

27. On numerous occasions beginning July 3, 2014 through August 4, 2014, Plaintiff Barbara Irwin caused her credit card to be swiped at a point-of-sale terminal operated by Jimmy John's so that she could complete purchases from Jimmy John's located in Arizona. From August 25, 2014 through September 2, 2014, Ms. Irwin was the direct victim of credit card fraud stemming from five fraudulent charges to the credit card that she used during the aforesaid transactions at Jimmy John's. Upon information and belief, the personal information and credit card data of Plaintiff Irwin used in this fraudulent charge was obtained as the result of Jimmy John's breach. As a result of the fraud, Ms. Irwin was subjected to expenses and the denial of the use of credit card she routinely used.

28. Plaintiff believed that Jimmy John's would maintain the personal and financial information contained on the financial cards used in their Jimmy John's purchases in a reasonably secure manner and provided their card to Jimmy John's on that basis. Had Plaintiff known that Jimmy John's would not maintain each of their information in a reasonably secure manner, she would not have allowed her financial cards to be swiped at The Company's point-of-sale terminal.

29. Plaintiff's personal information associated with each of their debit or credit cards was compromised in and as a result of Jimmy John's data breach. Plaintiff was harmed by having her financial and personal information compromised and faces the imminent and certainly

impending threat of future additional harm from the increased threat of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

CLASS ACTION ALLEGATIONS

30. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings her claims that the Company violated state data breach statutes (Count I) on behalf of separate statewide classes in and under the respective data breach statutes of the States of Alaska, Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia. These classes are defined as follows:

Statewide Data Breach Statute Classes:

All residents of [name of State or District of Columbia] who made an in-store purchase at Jimmy John's in the United States using a credit or debit card at any time between the beginning of the Data Breach through the period the breach was secured or September 24, 2104, whichever is later.

31. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings separate claims for breach of implied contract (Count II), bailment (Count III), unjust enrichment (Count IV), violation of the on the Arizona Consumer Fraud Act, A.R.S. 44-151, *et seq.*, and violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, on behalf of the respective statewide classes in and under the laws of each respective State of the United States and the District of Columbia as set forth in Counts II, III, IV, V, and VI. These classes for each of the foregoing claims are defined as follows:

Statewide [Breach of Implied Contract, Bailment or Unjust Enrichment] Class:

All residents of [name of State or District of Columbia] who made an in-store purchase at Jimmy John's in the United States using a credit or debit card at any time between the beginning of the Data Breach through the period the breach was secured or September 24, 2104, whichever is later.

32. Plaintiff further seeks to represent, and assert a claim for violation of the Arizona Consumer Fraud Act, A.R.S. 44-151, *et seq.* on behalf of, a subclass defined as:

All Class members who reside in the State of Arizona or made an in-store purchase at a Jimmy John's located in the State of Arizona using a debit or credit card (the "Arizona Subclass").

33. Plaintiff further seeks to represent, and assert a claim for violation of Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* on behalf of, a subclass defined as:

All Class members who reside in the State of Illinois or made an in-store purchase at a Jimmy John's located in the State of Illinois using a debit or credit card (the "Illinois Subclass").

34. Excluded from each of the above Classes are Jimmy John's, Inc., including any entity in which Jimmy John's has a controlling interest, is a parent or subsidiary, or which is controlled by Jimmy John's, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Jimmy John's. Also excluded are the judges and court personnel in this case and any members of their immediate families.

35. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class wide basis using the same exclusive and common evidence as would be used to prove those elements in individual actions alleging the same claims.

36. All members of the proposed Classes are readily ascertainable. Jimmy John's has access to addresses and other contact information for thousands of members of the Class, which can be used for providing notice to many Class members.

37. Numerosity. Plaintiff does not know the exact number of Class members but believe that the Class comprises thousands if not tens of thousands of consumers throughout these United States. As such, Class members are so numerous that joinder of all members is impracticable.

38. Commonality and predominance. Well-defined, nearly identical legal or factual questions affect all Class members. These questions predominate over questions that might affect individual Class members. These common questions include, but are not limited to, the following:

- a. Whether there was an unauthorized disclosure by Defendants of Class members' personal and/or financial information;
- b. Whether Defendants enabled an unauthorized disclosure of Class members' personal and/or financial information;
- c. Whether Defendants misrepresented the safety and security of Class members' personal and/or financial information maintained by Defendant;
- d. Whether Defendants implemented and maintained reasonable procedures and practices appropriate for maintaining the safety and security of Class members' personal and/or financial information;
- e. When Defendants became aware of an unauthorized disclosure of Class members' personal and/or financial information;
- f. Whether Defendants unreasonably delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;

- g. Whether Defendants intentionally delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;
- h. Whether Defendants' conduct was negligent;
- i. Whether Defendants' conduct was deceptive;
- j. Whether Defendants' conduct was knowing, willful, intentional, and/or malicious;
- k. Whether Defendants' conduct constitutes breach of an implied contract;
- l. Whether Defendants' violated the Stored Communications Act, 18.U.S.C. §2702;
- m. Whether Defendants violated the Arizona Consumer Fraud Act, A.R.S. 44-151, *et seq.*;
- n. Whether Defendants violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*; and
- o. Whether Plaintiff and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

39. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff and all Class members were injured through the Company's misconduct described above and assert the same claims for relief. The same events and conduct that give rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each Class member is a person that has suffered harm as a direct result of the same conduct (and omissions of material facts) engaged in by Jimmy John's and resulting in Jimmy John's data breach.

40. Adequacy. Plaintiff will fairly and adequately protect Class members' interests. Plaintiff has no interests antagonistic to Class members' interests, and Plaintiff has retained

counsel that has considerable experience and success in prosecuting complex class action and consumer protection cases.

41. Superiority. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiff and the Class members. Plaintiff and the Class members have been harmed by the Company's wrongful actions and inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to the Company's wrongful actions and inaction.

42. A class action is an appropriate method for the fair and efficient adjudication of this controversy. There is no special interest in the members of the Class individually controlling the prosecution of separate actions. The loss of money and other harm sustained by many individual Class members will not be large enough to justify individual actions, especially in proportion to the significant costs and expenses necessary to prosecute this action. The expense and burden of individual litigation makes it impossible for many members of the Class individually to address the wrongs done to them. Class treatment will permit the adjudication of claims of Class members who could not afford individually to litigate their claims against the Company. Class treatment will permit a large number of similarly situated persons to prosecute their common claims in a single form simultaneously, efficiently, and without duplication of effort and expense that numerous individual actions would entail. No difficulties are likely to be encountered in the management of this class action that would preclude its maintenance as a class action, and no superior alternative exists for the fair and efficient adjudication of this controversy. Furthermore, Jimmy John's transacts substantial business in and perpetuated its unlawful conduct in Arizona. Jimmy John's will not be prejudiced or inconvenienced by the maintenance of this class action in this forum.

43. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(3). The above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

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

45. The expense and burden of litigation will substantially impair the ability of Plaintiff and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Jimmy John's will retain the benefits of its wrongdoing despite its serious violations of the law.

COUNT I
Violations Of State Data Breach Statutes
(On behalf of Plaintiff and the separate statewide data breach statute classes.)

46. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

47. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedient time possible and without unreasonable delay.

48. Jimmy John's data breach constitutes a breach of the security system of the Company within the meaning of the below state data breach statutes and the data breached is protected and covered by the below data breach statutes.

49. Plaintiff's and Class members' names, credit and debit card numbers, card expiration dates, CVVs addresses, phone numbers and email addresses constitute personal information under and subject to the below state data breach statutes.

50. Jimmy John's unreasonably delayed in informing the public, including Plaintiff and members of the statewide Data Breach Statute Classes ("Class," as used in this Count I), about the breach of security of Plaintiff's and Class members' confidential and non-public personal information after Jimmy John's knew or should have known that the data breach had occurred.

51. Jimmy John's failed to disclose to Plaintiff and Class members without unreasonable delay and in the most expedient time possible, the breach of security of Plaintiff's and Class members' personal and financial information when the Company knew or reasonably believed such information had been compromised.

52. Plaintiff and members of the Class suffered harm directly resulting from the Company's failure to provide and the delay in providing Plaintiff and Class members with timely and accurate notice as required by the below state data breach statutes. Plaintiff suffered the damages alleged above as a direct result of the Company's delay in providing timely and accurate notice of the data breach.

53. Had Jimmy John's provided timely and accurate notice of the Company's data breach, Plaintiff and Class members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by the Company in providing notice. Plaintiff and Class members could have avoided making credit or debit card purchases at

the Company's stores, could have avoided shopping at the Company's stores at all, and could have contacted their banks to cancel their cards, or could otherwise have tried to avoid the harm caused by the Company's delay in providing timely and accurate notice.

54. The Company's failure to provide timely and accurate notice of Jimmy John's data breach violated the following state data breach statutes:

- a. Alaska Stat. Ann. § 45.48.010(a), et seq.;
- b. Ark. Code Ann. § 4-110-105(a), et seq.;
- c. Ariz. Rev. Stat. § 44-7501, et seq.;
- d. Cal. Civ. Code § 1798.83(a), et seq.;
- e. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;
- f. Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;
- g. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;
- h. D.C. Code § 28-3852(a), et seq.;
- i. Fla. Stat. Ann. § 501.171(4), et seq.;
- j. Ga. Code Ann. § 10-1-912(a), et seq.;
- k. Haw. Rev. Stat. § 487N-2(a), et seq.;
- l. Idaho Code Ann. § 28-51-105(1), et seq.;
- m. Ill. Comp. Stat. Ann. 530/10(a), et seq.;
- n. Iowa Code Ann. § 715C.2(1), et seq.;
- o. Kan. Stat. Ann. § 50-7a02(a), et seq.;
- p. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;
- q. La. Rev. Stat. Ann. § 51:3074(A), et seq.;
- r. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;

- s. Mass. Gen. Laws Ann. Ch. 93H § 3(a), et seq.;
- t. Mich. Comp. Laws Ann. § 445.72(1), et seq.;
- u. Minn. Stat. Ann. § 325E.61(1)(a), et seq.;
- v. Mont. Code Ann. § 30-14-1704(1), et seq.;
- w. Neb. Rev. Stat. Ann. § 87-803(1), et seq.;
- x. Nev. Rev. Stat. Ann. § 603A.220(1), et seq.;
- y. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;
- z. N.J. Stat. Ann. § 56:8-163(a), et seq.;
- aa. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;
- bb. N.D. Cent. Code Ann. § 51-30-02, et seq.;
- cc. Okla. Stat. Ann. Tit. 24 § 163(A), et seq.;
- dd. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;
- ee. Pa. 73 Stat. § 2301, et sq.;
- ff. R.I. Gen. Laws Ann. § 11-49.2-3(a), et seq.;
- gg. S.C. Code Ann. § 39-1-90(A), et seq.;
- hh. Tenn. Code Ann. § 47-18-2107(b), et seq.;
- ii. Tex. Bus. & Com. Code Ann. § 521.053(b), et seq.;
- jj. Utah Code Ann. § 13-44-202(1), et seq.;
- kk. Va. Code. Ann. § 18.2-186.6(B), et seq.;
- ll. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;
- mm. Wis. Stat. Ann. § 134.98(2), et seq.; and
- nn. Wyo. Stat. Ann. § 40-12-502(a), et seq.

55. Plaintiff and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to a) damages suffered by Plaintiff and Class members as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the separate statewide breach of implied contract classes.)

56. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

57. When Plaintiff and members of the Breach of Implied Contract Classes (“Class” as used in this Count II) provided their financial and personal information to Jimmy John’s in order to make purchases at the Company’s stores, Plaintiff and members of the Class entered into implied contracts with the Company pursuant to which the Company agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

58. Jimmy John’s solicited and invited Plaintiff and members of the Class to purchase products at Jimmy John’s stores using their credit or debit cards. Plaintiff and members of the Class accepted the Company’s offers and used their credit or debit cards to purchase products at the Company’s stores during the period of the Company’s data breach.

59. Each purchase made at a Jimmy John’s store by Plaintiff and members of the Class using their credit or debit card was made pursuant to the mutually agreed upon implied contract with the Company under which the Company agreed to safeguard and protect Plaintiff’s and Class members’ personal and financial information, including all information contained in the magnetic

stripe of Plaintiff's and Class members' credit or debit cards, and to timely and accurately notify them that such information was compromised and breached.

60. Plaintiff and Class members would not have provided and entrusted their financial and personal information, including all information contained in the magnetic stripes of their credit and debit cards, to Jimmy John's in order to purchase products at the Company's stores in the absence of the implied contract between them and the Company.

61. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Jimmy John's.

62. Jimmy John's breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the personal and financial information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of the Company's data breach.

63. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of The Company's breaches of the implied contracts between Jimmy John's and Plaintiff and members of the Class.

64. Wherefore, Plaintiff prays for relief as set forth below.

COUNT III
Bailment

(On behalf of Plaintiff and the separate statewide bailment classes.)

65. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

66. Plaintiff and members of the separate statewide Bailment Classes ("Class" as used in this Count III) delivered their personal and financial information, including the information

contained on the magnetic stripes of their credit or debit cards, to Jimmy John's for the exclusive purpose of making purchases from the Company at the Company's stores.

67. In delivering their personal and financial information to Jimmy John's, Plaintiff and Class members intended and understood that the Company would adequately safeguard their personal and financial information.

68. Jimmy John's accepted possession of Plaintiff's and Class members' personal and financial information for the purpose of accepting payment for goods purchased by Plaintiff and members of the Class at the Company's stores.

69. By accepting possession of Plaintiff's and Class members' personal and financial information, Jimmy John's understood that Plaintiff and Class members expected the Company to adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

70. During the bailment (or deposit), Jimmy John's owed a duty to Plaintiff and Class members to exercise reasonable care, diligence and prudence in protecting their personal and financial information.

71. Jimmy John's breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' personal and financial information.

72. Jimmy John's further breached its duty to safeguard Plaintiff's and Class members' personal and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the Company's data breach.

73. Jimmy John's failed to return, purge or delete the personal and financial information of Plaintiff and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

74. As a direct and proximate result of the Company's breach of its duty, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Jimmy John's, including but not limited to the damages set forth above.

75. As a direct and proximate result of the Company's breach of its duty, the personal and financial information of Plaintiff and Class members entrusted to Jimmy John's during the bailment (or deposit) was damaged and its value diminished.

76. Wherefore, Plaintiff prays for relief as set forth below.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiff and the separate statewide unjust enrichment classes.)

77. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

78. Plaintiff and members of the separate statewide Unjust Enrichment Classes ("Class" as used in this Count IV) conferred a monetary benefit on Jimmy John's in the form of monies paid for the purchase of goods from Jimmy John's during the period of Jimmy John's data breach.

79. Jimmy John's appreciates or has knowledge of the benefits conferred directly upon it by Plaintiff and members of the Class.

80. The monies paid for the purchase of goods by Plaintiff and members of the Class to Jimmy John's during the period of the Company's data breach were supposed to be used by the

Company, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and members of the Class.

81. Jimmy John's failed to provide reasonable security, safeguards and protection to the personal and financial information of Plaintiff and Class members and as a result, Plaintiff and Class members overpaid the Company for the goods purchased through use of their credit and debit cards during the period of the Company's data breach.

82. Under principles of equity and good conscience, Jimmy John's should not be permitted to retain the money belonging to Plaintiff and members of the Class, because the Company failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal and financial information that they paid for but did not receive.

83. As a result of the Company's conduct as set forth in this Complaint, Plaintiff and members of the Class suffered damages and losses as stated above, including monies paid for Jimmy John's products that Plaintiff and Class members would not have purchased had the Company disclosed the material fact that it lacked adequate measures to safeguard customers' data and had the Company provided timely and accurate notice of the data breach, and including the difference between the price they paid for the Company's goods as promised and the actual diminished value of its goods and services.

84. Plaintiff and the Class have conferred directly upon Jimmy John's an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiff and the Class.

85. The economic benefit, including the monies paid and the overcharges and profits derived by the Company and paid by Plaintiff and members of the Class, is a direct and proximate result of the Company's unlawful practices as set forth in this Complaint.

86. The financial benefits derived by the Company rightfully belong to Plaintiff and members of the Class.

87. It would be inequitable under established unjust enrichment principles in the District of Columbia and all of the 50 states for the Company to be permitted to retain any of the financial benefits, monies, profits and overcharges derived from The Company's unlawful conduct as set forth in this Complaint.

88. Jimmy John's should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by the Company.

89. A constructive trust should be imposed upon all unlawful or inequitable sums received by the Company traceable to Plaintiff and the Class.

90. Plaintiff and the Class have no adequate remedy at law.

91. Wherefore, Plaintiff prays for relief as set forth below.

COUNT V

**Violation of the Arizona Consumer Fraud Act, A.R.S. 44-151, *et seq.*
(On behalf of Plaintiff and the Arizona Subclass)**

92. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

93. Plaintiff asserts Count V on behalf of herself and the members of the Arizona Subclass.

94. Cashless purchases, including those made with a debit or credit card, comprise a significant portion of retail purchases, and enable retailers to maximize their sales by providing customers payment alternatives.

95. Jimmy John's offered and advertised its POS systems at each of the Jimmy John's location to induce the Plaintiff and members of the Arizona Subclass to make purchases from

Jimmy John's utilizing the POS. Jimmy John's intended for Plaintiff and the other members of the Arizona Subclass to rely on Jimmy John's to protect, secure, and prevent access from unauthorized third parties the personal and financial information furnished to it by Plaintiff and the Arizona Subclass in connection with their debit and credit card transactions.

96. Instead, Jimmy John's knowingly, and intentionally, maintained an insecure POS system that, along with inadequate oversight of its information systems, was inadequate to effectively protect Plaintiff and the Arizona Subclass members' financial and personal information from being compromised.

97. Jimmy John's either willfully failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring, and concealed, omitted and misrepresented this fact from Plaintiff and the Arizona Subclass.

98. Jimmy John's benefited from maintaining an insecure and susceptible POS system that exposed its customers' financial information to theft by not having to make significant one-time and going expenditures to purchase, implement and maintain adequate measures that that would have prevented the data from being compromised, or limited the extent of the breach through early detection.

99. Jimmy John's fraudulent and deceptive acts and omissions were intended to induce Plaintiff and the other Arizona Subclass members' reliance on Jimmy John's deception that their financial information was secure and protected when using debit and credit cards to make purchases from Jimmy John's.

100. Plaintiff and the members of the Arizona Subclass were deceived by Jimmy John's failure to properly implement adequate, commercially reasonable security measures to protect their private financial information.

101. Plaintiff and the Arizona Subclass were induced as a result of Defendants' unlawful conduct to use their credit or debit cards by utilizing Jimmy John's POS system in connection with the sale by Jimmy John's of its products to Plaintiff and the Arizona Subclass.

102. Jimmy John's violated A.R.S. § 44-1522(A) by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other Arizona Subclass members' private financial information.

103. Jimmy John's failure to maintain reasonable and appropriate means to protect consumers' personal and financial information, and failure to promptly notify consumers of the security breach, constitutes unfair acts or practices under Federal Trade Commission Act, 15 U.S.C. § 45(a) because substantial injury to Class members was not reasonably avoidable by consumers and is not offset by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n); A.R.S. § 44-1522(C).

104. Jimmy John's failure to promptly and adequately notify affected customers of the Data Breach also served as an unlawful practice as it failed to act in accordance with Illinois law that governed its corporate conduct as to all consumers.

105. Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*, provides:

Sec. 10. Notice of Breach.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

106. Jimmy John's violated 815 ILCS 530/10, as alleged herein. The violation of 815 ILCS 530/10 is deemed "an unlawful practice" under Illinois' Consumer Fraud and Deceptive Business Practices Act. 815 ILCS 530/20.

107. Plaintiff and the Arizona Subclass members have suffered injury in fact and actual damages.

108. It was foreseeable that Jimmy John's willful indifference or negligent course of conduct in handling its customers' personal and financial information would subject Plaintiff and the Arizona Subclass to risk that their information would be compromised by unscrupulous third parties, and Jimmy John's unlawful conduct did, in fact, result in the Data Breach which has harmed Plaintiff and the Arizona Subclass.

109. Plaintiff and the Arizona Subclass have suffered actual damages including, among others, monetary loss from unauthorized bank account withdrawals and credit card charges, incurred costs associated with the theft of their personal and financial information including costs associated with reporting of the fraud, obtaining replacement cards and payment means, costs incurred with the increased risk of identity theft including present and future costs of credit monitoring services, loss of use of their credit and debit cards, and loss of use and control of the property rights in their personal and financial information as a result of Jimmy Johns' violations of the Arizona Consumer Fraud Act.

110. The fraudulent and deceptive acts of Jimmy John's were the result of Jimmy John's wanton or reckless conduct and/or reckless indifference to the interest of others.

Accordingly, an award of punitive damages is appropriate.

111. Wherefore, Plaintiff prays for relief as set forth below.

COUNT VI
**Violation of the Illinois Consumer Fraud and
Deceptive Business Practices Act, 815 ILCS 505/1, et seq**
(On behalf of Plaintiff and the Illinois Subclass)

112. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

113. As a result of Jimmy John's unlawful conduct alleged herein, Jimmy John's violated 815 ILCS 505/1, *et seq.*, by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other Illinois Subclass members' private financial information, by violating 815 ILCS 530/10, as alleged herein which is itself deemed an "unlawful practice" under Illinois' Consumer Fraud and Deceptive Business Practices Act. 815 ILCS 530/20.

114. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein.

115. Wherefore, Plaintiff prays for relief as set forth below.

PRAYER FOR RELIEF

A. On behalf of herself and the Classes set forth above, Plaintiff requests the Court order relief and enter judgment against Defendant and enter an order:

B. certifying this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2) and (b)(3), and, pursuant to Fed. R. Civ. P. 23(g), appoint the named Plaintiff to be Class representative and their undersigned counsel to be Class counsel;

C. requiring Defendants to make whole any losses suffered by Plaintiff and Class members;

D. requiring Defendants to pay for three years of credit card fraud monitoring services;

E. enjoining Defendants from further engaging in the unlawful conduct complained of herein;

F. awarding Plaintiff and the Classes appropriate relief, including actual, statutory, and punitive damages, restitution and disgorgement;

G. awarding pre-judgment and post-judgment interest;

