IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF ILLINOIS

JOHN DRISCOLL, on behalf of himself and all others similarly situated,	)	
Plaintiffs,	)	Case No.: 3:15-cv-1089
vs.	)	**JURY TRIAL DEMANDED**
TRUMP INTERNATIONAL HOTELS MANAGEMENT LLC, d/b/a Trump Hotel Collection, a Delaware limited liability company,	)	
and	)	
JOHN DOES 1-20,	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff JOHN DRISCOLL, on behalf of himself and all others similarly situated ("Consumer Plaintiffs"), by and through their attorneys, John Hipskind and Brady McAninch, of the law firm of Hipskind & McAninch, LLC, bring this class action against TRUMP INTERNATIONAL HOTELS MANAGEMENT LLC, D/B/A TRUMP HOTEL COLLECTION ("Trump") and any other potentially responsible parties to be identified (sometimes collectively, the "Defendants").

INTRODUCTION AND NATURE OF ACTION

1. Consumer Plaintiffs bring this class action against Defendants for their failure to secure and safeguard the personal financial data, including, but not limited to, names, account numbers, expiration dates, PINs/security codes, and other numerical information (collectively, "Personal Identifying Information" or "PII") of individuals who used a payment card at several locations owned, operated, and/or managed by Defendants, including but not limited to Trump SoHo New York, Trump National Doral, Trump International New York, Trump International Chicago, Trump International Waikiki, Trump International Hotel & Tower Las Vegas, and Trump International Toronto (collectively the "Properties").

2. On or about September 29, 2015, Trump announced data thieves had gained unauthorized access to Consumer Plaintiffs' and other Class members' PII through the portion of its computer network that accepts or processes payment card transactions for the Properties. According to the announcement, between May 19, 2014 and June 2, 2015, the payment card data of customers at the Properties was subject to unauthorized malware access ("Data Breach").

3. Defendants' security failures enabled the hackers to access Consumer Plaintiffs' and the other Class members' PII from within Defendants' computer systems and put Consumer Plaintiffs' and the other Class members' financial information at serious, immediate, and ongoing risk. The practice with such data breaches is that hackers will continue to use the information they obtained as a result of inadequate security, as with Defendants, to exploit and injure consumers by selling the PII to third parties and otherwise using the PII for illicit purposes. That ongoing activity now blankets the Consumer Plaintiffs and the other Class members with a known and documented risk.

4. On information and belief, illicit websites are selling the stolen payment card PII "dumps" to international card counterfeiters and fraudsters, and issuing financial institutions are attempting to mitigate their risk. After purchasing Class members' PII, criminals can create counterfeit credit cards by encoding the stolen payment card PII onto any card with a magnetic stripe and can then use the counterfeit cards to make fraudulent purchases. Similarly, criminals can create fake debit cards with the stolen payment card PII, and withdraw cash from the bank accounts of unsuspecting victims through ATMs.

5. On or about July 1, 2015, data security journalist Brian Krebs reported that "sources at several banks [] traced a pattern of fraudulent debit and credit card charges to accounts that had all been used at Trump hotels . . . ," leading to the conclusion that Consumer Plaintiffs' and Class Members' PII has been obtained and is being fraudulently used by data thieves.[1]

6. On information and belief, the root cause of the Data Breach was Defendants' failure to fix elementary deficiencies in their security systems, abide by industry regulations, and

[1] http://krebsonsecurity.com/2015/07/banks-card-breach-at-trump-hotel-properties/

respond to other similar data breaches directed at retailers. In addition, on information and belief, Defendants failed to abide by best practices and industry standards. Had Defendants acted competently, criminals would have been unable to access the PII of Consumer Plaintiffs and the members of the Class.

7. In addition to failing to prevent the Data Breach, Defendants also failed to timely disclose the extent of the Data Breach, failed to individually notify Consumer Plaintiffs and Class members of the Data Breach in a timely manner, and failed to take other reasonable steps to clearly and conspicuously inform Consumer Plaintiffs and Class members of the nature and extent of the Data Breach. By failing to provide adequate notice, Defendants prevented Consumer Plaintiffs and Class members from protecting themselves from the consequences of the Data Breach.

8. Defendants' wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Consumer Plaintiffs' and Class members' PII constitute violations of state consumer protection laws and state data breach notification laws, negligence, negligence *per se*, breach of implied contract, and unjust enrichment.

9. Accordingly, Consumer Plaintiffs, individually and on behalf of all other members of the Class, asserts claims for violations of state consumer protection laws and state data breach notification laws, negligence, negligence *per se*, breach of implied contract, and unjust enrichment, and seek injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief authorized in equity or by law.

JURISDICTION AND VENUE

10. The Court has original jurisdiction pursuant to 28 U.S.C. § 1332. Plaintiff is a citizen of a state different than Defendant. Additionally, the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and is a class action in which there are in excess of 100 class members and many members of the Class are citizens of a state different from Defendant.

11. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(2) because a substantial part of the events or omissions giving rise to Consumer Plaintiffs' claims occurred in this

judicial district. Plaintiff Driscoll was solicited and encouraged within this district to transact business with Defendanats. Plaintiff Driscoll also established and maintains in this district the relevant accounts to which his payment cards are linked; experiences within this district the harms, losses, and damages accruing from the Data Breach; and will have to continuously undertake within this district remedial and protective action to attempt to safeguard himself from future losses and harms.

PARTIES

12. Plaintiff John Driscoll is a citizen of Illinois. During relevant times, Plaintiff Driscoll stayed at multiple of the Properties, including but not limited to Trump SoHo New York and Trump International Chicago. On information and belief, Plaintiff Driscoll's PII, including the full contents of the magnetic strip of his debit card, was compromised as a result of Defendants' security failure. When the Data Breach was announced, Plaintiff Driscoll spent time determining if his card was compromised including, but not limited to, reviewing information released about the Data Breach and the impacted locations. As a result of such compromise and theft, Plaintiff Driscoll suffered damages in an amount yet to be determined, as such damages are ongoing and include, but are not limited to, time spent monitoring his account information to guard against potential fraud.

13. As a direct and/or proximate result of Defendants' wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Consumer Plaintiffs' and the Class members' PII, Consumer Plaintiffs and the Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) invasion of privacy, (ii) breach of the confidentiality of their PII by Defendants' unauthorized release and disclosure, (iii) lost benefit of their bargain, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, (v) diminished value of PII protection services purchased from Defendants, (vi) the untimely and inadequate notification of the Data Breach, (vii) the resulting increased risk of future ascertainable losses, economic damages and other actual injury and harm, and (viii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and payment card accounts.

14. Defendant Trump International Hotels Management LLC is a Delaware limited liability company with its headquarters and principal place of business in New York, New York. Pursuant to 28 U.S.C. § 1332(10), defendant is deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized. Defendant is therefore a citizen of New York and Delaware. Service on Defendant may be had by way of its registered agent, National Registered Agents, Inc., 208 So. LaSalle Street, Suite 814, Chicago, Illinois, 60604. Upon information and belief, Defendant does business as Trump Hotel Collection.

15. On information and belief, several other corporations, companies, partnerships, joint ventures, business combinations, legal entities, and/or natural persons have ownership, control, management, or other interests in the Properties such that they are legally liable for the Data Breach and its resulting harms. Such entities are named herein as JOHN DOES 1-20.

FACTUAL BACKGROUND

I. The Breach.

16. Based on a public notice announcing the breach Trump published on September 29, 2015, and upon information and belief, from at least May 19, 2014 to June 2, 2015, unauthorized malware had access to payment card information as it was inputted into payment card systems at the Properties. This resulted in the compromise of payment card data (including payment card account number, card expiration date, and security code) of individuals who used a payment card at the Properties. For transactions at certain Properties, cardholder name and other PII may also have been compromised.

17. According to Trump, months elapsed between the time Consumer Plaintiffs' and Class members' PII was improperly accessed and the time Defendants disseminated notice of the unauthorized PII access. Defendants' unwarranted delay in notifying Consumer Plaintiffs and Class members about the unauthorized PII disclosure deprived them of the opportunity to take effective remedial action to reduce the short and long term risk of further fraudulent activity.

II. The Breach Was Entirely Avoidable and Foreseeable by Defendants.

18. On information and belief, Defendants should have foreseen the Data Breach

and prevented its occurrence because the deficiencies in Defendants' security system that allowed the Data Breach to occur, such as lack of 1) appropriate antivirus and malware detection software, 2) lockout controls and two factor authentication, 3) firewalls and appropriate network segmentation, 4) appropriate network intrusion detection and monitoring, and 5) sophisticated usernames and passwords, are elementary security measures that even the most inexperienced IT professional would identify as problematic.

19. These security flaws and other infirmities were explicitly outlined by Visa, as early as 2009, when it issued a Data Security Alert outlining the threat of RAM scraper malware.[2] The report instructs companies to "[s]ecure remote access connectivity," "[i]mplement a secure network configuration, including egress and ingress filtering to only allow the ports/services necessary to conduct business" (i.e., segregate networks), "actively monitor logs of network components, including IDS [intrusion detection systems] and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "[e]ncrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit" and "[w]ork with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration."

20. Despite the simplicity of these security flaws and Visa's warning about their existence and potential danger, Defendants failed to take any corrective action and instead neglected their network security and failed to protect Consumer Plaintiffs and the Class.

21. Second, Defendants' security flaws ran afoul of best practices and industry standards. If Defendants would have followed these practices and complied with industry standards the Breach would not have occurred.

[2] The Visa report can be found here: https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf (last visited June 24, 2015).

22. All merchants that accept customer payments via payment cards, including Defendants, are obligated and required to comply with the Payment Card Industry Data Security Standards (the "PCI DSS"). *How to Be Compliant: Getting Started with PCI Data Security Standard Compliance*, PCI SSC, *available at*. pcisecuritystandards.org/merchants/how_to_be_compliant.php (last visited June 24, 2015) (stating "[i]f you are a merchant that accepts payment cards, you are required to be complaint with the PCI [DSS]."). Compliance with the PCI DSS is common practice in the retail industry.

23. The PCI DSS, among other things, mandates merchants to protect cardholder data, PCI DSS v. 3.0 at 34 (Nov. 2013),[3] requires merchants to install and maintain firewalls, *id.* at 19, forbids merchants from using default settings and passwords for applications and devices, *id.* at 28, requires merchants to segment cardholder data, *id.* at 61, and requires merchants to identify and authenticate their system users. *Id.* at 64.

24. To adhere to the PCI DSS, a merchant must, *inter alia*:

> First, **Assess** -- identify cardholder data, take an inventory of your IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data. Second, **Remediate** -- fix vulnerabilities and do not store cardholder data unless you need it. Third, **Report** -- compile and submit required remediation validation records (if applicable), and submit compliance reports to the acquiring bank and card brands you do business with.

(emphasis in original). *How to Be Compliant: Getting Started with PCI Data Security Standard Compliance*, PCI SSC, *available at* https://www.pcisecuritystandards.org/merchants/how_to_be_compliant.php (last visited June 24, 2015).

25. Despite these well-documented and well-known industry restrictions and mandates, Defendants failed to properly secure their systems to protect cardholder data. Had Defendants taken their obligations seriously, the breach would not have occurred.

---

[3] A copy of PCI DSS v. 3.0 can be found at: https://www.pcisecuritystandards.org/security_standards/documents.php?agreements=pcidss&association=pcidss (last visited June 24, 2015).

26. Despite the fact that Defendants were on notice of the very real possibility of consumer data theft associated with their security practices and despite the fact that Defendants knew or, at the very least, should have known, about the elementary infirmities associated with their security systems, they still failed to make any changes to their security practices and protocols. Consequently, hackers were able to access Consumer Plaintiffs' and Class members' PII with ease.

27. As a result of Defendants' indifference to the sensitive nature of Consumer Plaintiffs' and Class members' PII, both in Defendants' failure to employ adequate security measures and Defendants' failure to delete promptly its customers' sensitive data, PII of Consumer Plaintiffs and the Class has been exposed to criminals. This exposure has made the financial accounts of Consumer Plaintiffs and the members of the Class less secure and has subjected them to an imminent and real possibility of identity theft.[4]

28. In allowing and making possible the theft of Consumer Plaintiffs' and the other Class members' PII, Defendants failed to meet the standards of commercially reasonable steps that should be taken to protect Consumer Plaintiffs and the Class. Despite being obligated to do so, Defendants failed to employ appropriate technical, administrative, or physical procedures to protect the PII of Consumer Plaintiffs and the Class from unauthorized capture, dissemination, or misuse, thereby making Consumer Plaintiffs and the other Class members easy targets for theft and misuse of their financial information, including in the manner undertaken by the hackers here.

III. The Personal Information and Privacy of Consumers is Valuable.

29. The PII of Consumer Plaintiffs and the Class is a valuable property right. *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a

[4] Indeed, stolen information is often used well after the data breach in question. Recently, thieves attempted to charge thousands of dollars to a credit card that was compromised in the Home Depot data breach more than a year prior. *See* Stephen Montemayor, "Eagan woman, Chicago man accused of using stolen credit card numbers", *available at* http://www.startribune.com/eagan-woman-chicago-accused-of-using-credit-card-numbers-compromised-in-home-depot-data-breach/308201391/ (last visited June 24, 2015).

level comparable to the value of traditional financial assets.") (citations omitted). In fact, PII—including Consumer Plaintiffs' names combined with the payment card information disclosed and compromised in the Data Breach—is so valuable to fraudsters that they often buy and sell the information on the well-established national and international "cyber black-market" for years.

30. At a Federal Trade Commission ("FTC") public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's PII:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.

FTC Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, *available at* https://www.ftc.gov/sites/default/files/documents/public _events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited June 24, 2015). Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States. *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (online) *available at* http://www.wsj.com/articles/SB10001424052748703529004576160764037920274 (last visited June 24, 2015).

31. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit.

Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), *available at*

https://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/privacyroundtable_dec2009_transcript.pdf (last visited June 24, 2015).

32. Recognizing the high value consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated. Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited June 24, 2015).

33. This business has created a new market for the sale and purchase of this valuable data. *See Web's Hot New Commodity: Privacy*, *available at* http://online.wsj.com/news/articles/SB10001424052748703529004576160764037920274 (last visited June 24, 2015).

34. Consumers place a high value on their PII, as well as on the *privacy* of their PII. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49–44.62." Il-Horn Hann *et al.*, *The Value of Online Information Privacy* (Oct. 2002) *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited June 24, 2015); *see also* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) Information Systems Research 254, 254 (June 2011).

35. When consumers were surveyed about how much value they place on protecting their PII against improper access and unauthorized secondary use—two concerns at issue here—they valued the restriction of improper access at between $11.33 and $16.58 per website, and valued the prohibition of secondary use at between $7.98 and $11.68 per website. *Id.*

36. The value of the PII of Consumer Plaintiffs and the Class on the cyber black market is substantial—credit card numbers alone range in cost from $1.50 to nearly $100 per card

number. *The Cyber Black Market: What's Your Bank Login Worth*, *available at* http://www.ribbit.net/frogtalk/id/50/the-cyber-black-market-whats-your-bank-login-worth (last visited June 24, 2015); National Counterintelligence and Security Center, *How Much Do You Cost on the Black Market*, *available at* http://www.ncix.gov/issues/cyber/identity_theft.php (last visited June 24, 2015).

37. By virtue of the Data Breach and unauthorized release and disclosure of the PII of Consumer Plaintiffs and the Class, Defendants have deprived Consumer Plaintiffs and the Class of the substantial values of their PII, to which they are entitled.

IV. Data Breaches Lead to Identity Theft and Cognizable Injuries.

38. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

39. For example, The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name. *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), *available at* http://www.gao.gov/assets/270/262899.pdf (last visited June 24, 2015). The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name." *Id.*

40. According to the Federal Trade Commission ("FTC"), unauthorized PII disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), *available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf

(last visited June 24, 2015). Criminals use compromised PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

41. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

42. Indeed, the information identity thieves obtain from breaching corporate networks is so valuable that identify thieves often trade the information on the cyber black market for a number of years after the initial theft.

43. As a result, victims suffer immediate and long lasting exposure and are susceptible to further injury over the passage of time.

44. Most high profile data breaches, including those associated with the TJX Companies and Target, imminently and inevitably lead to identity theft and adverse use of PII, and the very real possibility of theft and adverse use continues into the future, long after the initial breach.

45. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

46. "The continuation of data breaches at the retail or POS level is becoming the favored target for hackers and thieves and these breaches are at epidemic proportions," says Richard Blech, CEO of Proximity. Tara Seals, *Security Researchers: Supervalu PoS Breach "Completely Avoidable"* (Aug. 21, 2014), available at http://www.infosecurity-magazine.com/news/security-researchers-supervalu-pos/ (last visited June 24, 2015).

47. Recent data breaches at Home Depot, Target, Neiman Marcus, Michaels, Sally Beauty, and eBay all underscore the fact that "criminals can rather easily leverage existing security weaknesses in corporate networks to gain access to sensitive data and critical PoS systems without

being detected." *Id*. As a result, "[n]ot making changes to account for this given the ongoing tsunami of headlines about such breaches is equivalent to pure negligence" in the view of some experts. *Id*.

48. The fact that these and other high-volume data breaches have been occurring for years underscores the care and attention Defendants should have given to the matter—but, unfortunately did not.

V. Consumer Plaintiffs and Class Members Have Suffered Ascertainable Losses, Economic Damages and Other Actual Injury and Harm.

49. As a direct and proximate result of Defendants' wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Consumer Plaintiffs' and other Class Members' PII, Consumer Plaintiffs and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) diminished value of their PII, (ii) the untimely and inadequate notification of the Data Breach, (iii) the resulting increased risk of future ascertainable losses, economic damages and other actual injury and harm, and (iv) the opportunity cost and value of lost time they must spend to monitor their financial accounts and payment card accounts—for which they are entitled to compensation.

CLASS DEFINITION AND ALLEGATIONS

50. Plaintiffs bring this action on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following three (3) multi-state classes:

> All persons who engaged in payment card transactions at Defendants' Properties, whose Personal Information was subject to Defendant's security failures and who suffered damages in the loss of time and use of their credit and debit cards until such time as replacement cards could be obtained.
>
> All persons who engaged in payment card transactions at Defendants' Properties, whose Personal Information was subject to Defendant's security failures and who suffered damages in the amount of fraudulent charges / unauthorized withdrawals made to their credit and/or debit cards or suffered damages in the amount of overdraft charges made to their credit and/or debit cards.

> All persons who engaged in payment card transactions at Defendants' Properties, whose Personal Information was subject to Defendant's security failures and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Defendant's security failures.

Excluded from the Classes are: (i) Defendants and their officers, directors, affiliates, parents, and subsidiaries (ii) all Class Members who timely and validly request exclusion from the Class, (iii) the Judge presiding over this action, and (iv) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches or who pleads *nolo contendere* to any such charge.

51. Certification of Consumer Plaintiffs' claims for class-wide treatment is appropriate because Consumer Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

52. The members of the Classes are so numerous that joinder of all members of the Classes is impracticable. Consumer Plaintiffs are informed and believe that the proposed Classes contain thousands of purchasers who used payment cards to complete purchases at Defendants' Properties who have been damaged by Defendants' conduct as alleged herein. The precise number of Class members is unknown to Consumer Plaintiffs, but may be ascertained from Defendants' records.

53. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

(1) whether Defendants engaged in the wrongful conduct alleged herein;

(2) whether the alleged conduct constitutes violations of the laws asserted;

(3) whether Defendants owed Consumer Plaintiffs and the other Class members a duty to adequately protect their personal and financial data;

(4) whether Defendants breached their duty to protect the personal and financial data of Consumer Plaintiffs and the other Class members;

(5) whether Defendants knew or should have known about the inadequacies of their payment processing network and the dangers associated with storing sensitive cardholder information;

(6) whether Defendants failed to use reasonable care and commercially reasonable methods to safeguard and protect Consumer Plaintiffs' and the other Class members' PII from unauthorized release and disclosure;

(7) whether the proper data security measures, policies, procedures and protocols were in place and operational within Supervalu's computer systems to safeguard and protect Consumer Plaintiffs' and the other Class members' PII from unauthorized release and disclosure;

(8) whether Defendants' conduct was the proximate cause of Consumer Plaintiffs' and the other Class members' injuries;

(9) whether Defendants took reasonable measures to determine the extent of the Data Breach after it was discovered;

(10) whether Defendants' delay in informing Consumer Plaintiffs and the other Class members of the Data Breach was unreasonable;

(11) whether Defendants' method of informing Consumer Plaintiffs and the other Class members of the Data Breach was unreasonable;

(12) whether Consumer Plaintiffs and the other Class members suffered ascertainable and cognizable injuries as a result of Defendants' conduct;

(13) whether Defendants' conduct was deceptive, unfair, or unconscionable, or constituted unfair competition;

(14) whether Defendants' conduct was likely to deceive a reasonable consumer;

(15) whether Consumer Plaintiffs and the other Class members are entitled to recover actual damages and/or statutory damages; and

(16) whether Consumer Plaintiffs and the other Class members are entitled to other appropriate remedies, including corrective advertising and injunctive relief.

54. Defendants engaged in a common course of conduct giving rise to the claims asserted by Consumer Plaintiffs, on behalf of themselves and the other Class members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

55. Consumer Plaintiffs' claims are typical of the claims of the members of the Classes because, inter alia, all Class members were injured through the uniform misconduct described above. Consumer Plaintiffs are advancing the same claims and legal theories on behalf of

themselves and all members of the Classes.

56. Consumer Plaintiffs will fairly and adequately protect the interests of the members of the Classes, have retained counsel experienced in complex consumer class action litigation, and intend to prosecute this action vigorously. Consumer Plaintiffs have no adverse or antagonistic interests to those of the Classes.

57. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

58. Consumer Plaintiffs seek preliminary and permanent injunctive and equitable relief on behalf of the Classes, preventing Defendants from further engaging in the acts described and requiring Defendants to provide full restitution to Consumer Plaintiffs and the other Class members.

59. Unless the Classes are certified, Defendants will retain monies received as a result of their conduct that were taken from Consumer Plaintiffs and the other Class members. Unless Class-wide injunctions are issued, Defendants will continue to commit the violations alleged, and the members of the Classes and the general public will continue to be deceived and injured.

60. Defendants have acted and refused to act on grounds generally applicable to the Classes, making appropriate final injunctive relief with respect to the Classes as a whole.

FIRST CAUSE OF ACTION
(State Consumer Protection Laws)

61. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

62. Consumer Plaintiffs and members of the Classes are consumers who used their credit and/or debit cards to purchase products from Defendants, primarily for personal, family or household purposes.

63. Defendants engaged in the conduct alleged above in transactions intended to result, and which did result, in the sale of goods and services to consumers, including Consumer Plaintiffs and the Class.

64. This course of conduct also affects trade and commerce, nationally and in Illinois. Defendants' actions and/or inactions regarding their failure to adequately protect the PII of Consumer Plaintiffs and the Class constitute deceptive acts and unfair practices and have a direct and substantial affect in Illinois and throughout the United States.

65. Defendants' conduct as alleged herein, including without limitation, Defendants' failure to maintain reasonable and adequate computer systems and data security practices, Defendants' fraudulent and deceptive omissions and/or misrepresentations regarding the security measures put in place to protect the PII of Consumer Plaintiffs and the Class and the lack of efficacy of these security measures, Defendants' failure to timely and accurately disclose the Breach to Consumer Plaintiffs and the Class, and Defendants' continued acceptance of credit and debit card information as payment for goods and services after Defendants knew or should have known of the Breach's occurrence and before Defendants fixed the problems that allowed for the Breach and purged their systems of the malicious hacker software, constitute unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices in violation of The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Stat. § 510/2(a)(5), (7) and (12), *et seq.*, as well as the similar laws of the various other states as they may appear.

66. Defendants' conduct has violated the state consumer protection laws

prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another, and/or "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;" and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

67. As a result, Defendants' conduct damaged Consumer Plaintiffs and the other members of the Class, who would not have otherwise completed credit and/or debit card purchases/transactions at Defendants' Properties, by exposing their information to third-party hackers.

68. Consumer Plaintiffs bring this action on behalf of themselves and all similarly situated persons for the requested relief and for the public benefit at large in order to promote truthful, honest and non-deceptive business practices, which will allow consumers to make informed purchasing decisions and to protect, Consumer Plaintiffs, members of the Class and the public from Defendants' unfair, deceptive, fraudulent, unconscionable and/or unlawful practices and methods of competition. Defendants' conduct as alleged herein has had widespread negative consequences and has affected consumers throughout the nation.

SECOND CAUSE OF ACTION
(State Data Breach Notification Statutes)

69. Consumer Plaintiffs incorporate by reference and reasserts all previous paragraphs.

70. The Data Breach constitutes a breach of Defendants' computer security systems within the meaning of the state data breach notifications statutes of several states as they may appear, and the data accessed in the Data Breach was protected and covered by the same.

71. The names, account numbers, expiration dates, PINs, and other numerical information of the Consumer Plaintiffs and the Class constitute personal information as defined by the state data breach notification statutes of several states as they may appear.

72. Defendants unreasonably delayed notification of the Data Breach, including the unauthorized access and theft of the PII of their customers, including Consumer Plaintiffs and the Classes, after Defendants knew or should have known that the Data Breach had occurred.

73. When the Data Breach began on or about May 19, 2014, Defendants did not disclose or notify the public of the data breach. Defendants knew or should have known that the Data Breach was occurring as early as May 19, 2014, but failed to disclose its existence to the public, including Consumer Plaintiffs and the Class, at this time.

74. From June 2, 2015, until around September 29, 2015, for a period of about four months, Defendants took inadequate action to remedy the Data Breach. Defendants failed to inform the public of the Data Breach during this time even though Defendants knew or should have known of the Data Breach's occurrence and the attendant unauthorized access, theft and dissemination of Consumer Plaintiffs' and the other Class members' PII.

75. On or around June 2, 2015, when Defendants finally reacted to the Data Breach and began purging its systems of the malicious hacker software and fixing the unreasonable security holes that led to the Data Breach, Defendants still failed to disclose or provide notice to the public that the Data Breach had occurred.

76. Defendants waited until around September 29, 2015, almost four months after discovery, to disclose the Data Breach and notify their customers. Defendants downplayed the significance of the Data Breach and claimed that they did not know whether Personal Information was stolen and that there was no evidence of misuse of any customer Personal Information.

77. Defendants failed to disclose to Consumer Plaintiffs and the other Class members, without unreasonable delay and in the most expedient time possible, the Data Breach and the unauthorized access and theft of the PII of Consumer Plaintiffs and the other Class members when Defendants knew, should have known, or reasonably believed that such information had been compromised.

78. On information and belief, no law enforcement agency instructed Defendants to withhold notification and disclosure of the Data Breach.

79. As a result of Defendants' failure to notify in the statutorily prescribed time periods, Consumer Plaintiffs and the other Class members suffered the direct harm as alleged above.

80. Had Defendants provided timely and accurate notice, Consumer Plaintiffs and members of the Class could have taken steps to mitigate the direct harm suffered as a result of Defendant's unreasonable and untimely delay in providing notice. Consumer Plaintiffs and the other members of the Class could have used cash instead of credit and debit cards in closing commercial transactions at Defendants' Properties, avoided shopping at the Properties altogether, contacted their financial institutions to cancel cards and accounts, or taken other steps in efforts to avoid the direct harm caused by Defendants' failure to notify.

81. Defendants' failure to notify Consumer Plaintiffs and the other Class members violated Ill. Comp. Stat. Ann. 530/10(a), *et seq.*, and the data breach notification statutes of other states as they may appear.

82. Consumer Plaintiffs and the other members of the Class seek all remedies available under the applicable state data breach notification statutes, including but not limited to damages as alleged above, equitable relief and reasonable attorneys' fees, and costs, as provided by law.

THIRD CAUSE OF ACTION
(Negligence)

83. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

84. A special relationship exists between Defendants and the Consumer Plaintiffs and the Classes. Defendants actively solicited Consumer Plaintiffs and the other Class members to use their PII in commercial transactions at Defendants' Properties. When Consumer Plaintiffs and the other Class members gave their PII to Defendants to facilitate and close commercial transactions, they did so with the mutual understanding that Defendants had reasonable security measures in place and Defendants would take reasonable steps to protect and safeguard the PII of Consumer Plaintiffs and the other Class members. Consumer Plaintiffs and the other Class members also gave their PII

to Defendants on the premise that Defendants were in a superior position to protect against the harms attendant to unauthorized access, theft and misuse of that information.

85. Upon gaining access to the PII of Consumer Plaintiffs and members of the Class, Defendants owed to Consumer Plaintiffs and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed and misused by unauthorized parties. Pursuant to this duty, Defendants were required to design, maintain and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Consumer Plaintiffs and the Class. Defendants further owed to Consumer Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

86. Defendants owed this duty to Consumer Plaintiffs and the other Class members because Consumer Plaintiffs and the other Class members compose a well-defined, foreseeable and probable class of individuals whom Defendants should have been aware could be injured by Defendants' inadequate security protocols. Defendants actively solicited Consumer Plaintiffs and the other Class members to use their PII in sales transactions at Defendants' Properties. To facilitate and close these sales transactions, Defendants used, handled, gathered and stored the PII of Consumer Plaintiffs and the other Class members. Attendant to Defendants' solicitation, use and storage, Defendants knew of their inadequate and unreasonable security practices with regard to their computer systems and also knew that hackers routinely attempt to access, steal and misuse the PII that Defendants actively solicited, used and/or stored from Consumer Plaintiffs and the other Class members. As such, Defendants knew a breach of their systems would cause damage to their customers, including Consumer Plaintiffs and the other Class members. Thus, Defendants had a duty to act reasonably in protecting the sensitive information of their consumers.

87. Defendants also owed this duty to Consumer Plaintiffs and the other Class members because Consumer Plaintiffs and members of the Class entrusted Defendants with their PII by making purchases with their credit and debit cards at Defendants' Properties. Defendants knew,

or should have known, of the risk inherent in obtaining, using, handling and/or storing the PII of Consumer Plaintiffs and the other Class members and of the critical importance in providing adequate security systems to protect such information while it is being gathered, used and stored.

88. Defendants also owed a duty to timely and accurately disclose to Consumer Plaintiffs and the other Class members the scope, nature and occurrence of the Breach. This duty was required and necessary in order for Consumer Plaintiffs and the other Class members to take appropriate measures to avoid unauthorized charges to their credit-and/or debit-card accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Defendants' unreasonable misconduct.

89. Defendants breached their duties to Consumer Plaintiffs and the other Class members by failing to implement and maintain security systems and controls that were capable of adequately protecting the PII of Consumer Plaintiffs and the other Class members. More specifically, Defendants breached their duties to Consumer Plaintiffs and the other Class members by failing to remedy the deficiencies found in the remote access points to their servers and corporate networks and by storing Consumer Plaintiffs' and the other Class members' data on their servers.

90. Defendants further breached their duties to Consumer Plaintiffs and the other Class members when they failed to fix the deficiencies associated with their security and storage policies despite the fact that they knew or, at the very least, should have known, that these deficiencies were the leading cause of data breaches and theft of sensitive consumer information.

91. Defendants also breached their duties to timely and accurately disclose to the Consumer Plaintiffs and the other Class members that their PII had been or was reasonably believed to have been improperly accessed or stolen.

92. Defendants' negligence in failing to exercise reasonable care in protecting the PII of Consumer Plaintiffs and the other Class members is further evidenced by Defendants' failures to comply with legal obligations and industry standards, such as the PCI DSS, and the delay between

the start of the Data Breach and the time when the Data Breach was disclosed.

93. The injuries to Consumer Plaintiffs and the other Class members were reasonably foreseeable to Defendants because laws, statutes, and industry standards, such as the PCI DSS, require Defendants to safeguard and protect their computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Consumer Plaintiffs' and the other Class members' PII.

94. The injuries to Consumer Plaintiffs and the other Class members also were reasonably foreseeable because Defendants knew or should have known that their computer systems used for processing consumer sales transactions were inadequate and unable to protect solicited consumer PII from being breached, accessed and stolen by hackers and unauthorized third parties. As such, Defendants' own misconduct created a foreseeable risk of harm to Consumer Plaintiffs and the other Class members.

95. Defendants' failure to take reasonable steps to protect the PII of Consumer Plaintiffs and the other members of the Class was a proximate cause of their injuries because it directly allowed hackers easy access to Consumer Plaintiffs' and the other Class members' PII. This ease of access allowed hackers to implement unsophisticated attacks and thereafter steal PII of Consumer Plaintiffs and the other members of the Class and disseminate it over black markets.

96. As a direct proximate result of Defendants' conduct, Consumer Plaintiffs and the other Class members have suffered theft of their PII. Defendants allowed cybercriminals access to Class members' PII, thereby decreasing the security of Class members' bank accounts, making Class members' identities less secure and reliable, and subjecting Class members to the imminent threat of identity theft. Not only will Consumer Plaintiffs and the other members of the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against the specter of identity theft for years to come.

97. Defendants' conduct warrants moral blame because Defendants actively solicited, used, handled and/or stored the PII of Consumer Plaintiffs and the other Class members without disclosing that their computer systems used for consumer transactions were inadequate and

unable to protect the PII of Consumer Plaintiffs and the other Class members.

98. Holding Defendants accountable under negligence law will further the policies embodied in such law by incentivizing larger property and/or hotel chains to properly secure sensitive consumer information and thereby protect the consumers who rely on these companies every day.

FOURTH CAUSE OF ACTION
(Breach of Implied Contract)

99. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

100. Defendants actively solicited the PII of Consumer Plaintiffs and members of the Classes by offering Consumer Plaintiffs and the other Class members the option of purchasing products or services at Defendants' Properties through use of credit and/or debit cards. Consumer Plaintiffs and the other members of the Class accepted Defendants' offers and used their credit and/or debit cards to purchase products or services at Defendants' Properties.

101. Each purchase that involved use of a credit or debit card was made pursuant to mutually agreed upon implied contract terms that Defendants would take reasonable measures to protect the PII of Consumer Plaintiffs and the other Class members and that Defendants would timely and accurately notify Consumer Plaintiffs and the other Class members if and when such information was compromised.

102. Had such implied contractual terms failed to exist, Consumer Plaintiffs and the other Class members never would have used their credit and debit cards to make purchases at Defendants' Properties and never would have entrusted their PII to Defendants for use.

103. Consumer Plaintiffs and the other Class members fully performed their obligations under the implied contractual terms.

104. In contrast, Defendants breached the implied terms of the contracts they made with Consumer Plaintiffs and the other Class members by failing to reasonably protect their PII and by failing to provide adequate notice of the Data Breach and unauthorized access of such

information.

105. The damages described herein and suffered by Consumer Plaintiffs and the other Class members were the direct proximate result of Defendant's breach of the implied contractual terms.

FIFTH CAUSE OF ACTION
(Negligence Per Se)

106. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

107. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits "unfair . . . practices in or affecting commerce" including, as recently interpreted by the FTC, the act or practice by retailers, such as Defendants, of failing to take reasonable measures to protect their customers' PII.

108. Defendants violated Section 5 and similar state statues by failing to employ reasonable security systems, controls and procedures to protect the PII of Consumer Plaintiffs and the other Class members. This violation constitutes negligence *per se*.

109. The Consumer Plaintiffs and the statewide Negligence *Per Se* Class are the individuals the FTC Act seeks to protect. For instance, the FTC Act expressly prohibits "unfair" acts that "cause or are likely to cause substantial injury to ***consumers*** which is not reasonably avoidable by ***consumers***."

110. Additionally, the harm that has occurred to Consumer Plaintiffs and the other Class members is the type of harm the FTC Act was intended to prevent and remedy. To be sure, the FTC has pursued a number of enforcement actions against businesses that caused the unauthorized dissemination, collection and/or use of their customers' PII as a result of the businesses' lack of reasonable and adequate security measures and practices.

111. As a direct and proximate result of Defendants' negligence *per se*, the Consumer Plaintiffs and the other Class members have suffered injury and damages as described herein.

112. Defendants' violation of Section 5 of the FTC Act thus constitutes negligence *per se* and Consumer Plaintiffs and the other Class members are entitled to recover damages in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
(Unjust Enrichment)

113. Consumer Plaintiffs incorporate by reference and reassert all previous paragraphs.

114. Consumer Plaintiffs and members of the Classes conferred a monetary benefit on Defendants in the form of money paid for the purchase of goods or services from Defendants.

115. Defendants appreciate or have knowledge of the benefits conferred directly upon them by Consumer Plaintiffs and the other members of the Class.

116. Defendants knew or should have known about the Data Breach and but for their inadequate security practices, would have known about the Data Breach on its original date of occurrence.

117. Had Consumer Plaintiffs and the other Class members known about the Data Breach, they would not have patronized Defendants' Properties and would not have conferred upon Defendants monetary benefits.

118. Thus, had Consumer Plaintiffs and the other Class members been alerted to the Data Breach by Defendants, who knew or should have known, they would not have patronized Defendants' Properties and purchased goods or services from Defendants.

119. The financial benefits of money paid by Consumer Plaintiffs and the other Class members and the profits derived therefrom are a direct and proximate result of Defendants' unlawful and negligent practices and Defendants' failure to notify Consumer Plaintiffs and the other Class members of the Breach.

120. These financial benefits rightfully belong to the Consumer Plaintiffs and the other Class members and it would be inequitable under unjust enrichment principles for Defendants to retain any of the financial benefits they would not have received but-for their illegal and uncaring

conduct.

121. As such, Defendants should be compelled to disgorge all inequitable proceeds to Consumer Plaintiffs and the other Class members by way of a common fund for their benefit.

122. A constructive trust should be imposed to recoup the inequitable sums received by Defendants and traceable to Consumer Plaintiffs and the other Class members.

PRAYER FOR RELIEF

Wherefore, Consumer Plaintiffs pray for a judgment:

1. Certifying the Class(es) as requested herein;

2. Awarding Consumer Plaintiffs and the proposed Class members damages;

3. Awarding restitution and disgorgement of Defendants' revenues to Consumer Plaintiffs and the proposed Class members;

4. Awarding consequential damages for time and money spent by Consumer Plaintiffs and the other members of the Class in response to Defendants' improper release and dissemination of their PII;

5. Awarding injunctive relief as permitted by law or equity, including:

   a. Enjoining Defendants from continuing the unlawful practices as set forth herein;

   b. Directing Defendants to identify, with Court supervision, victims of their conduct and pay them all money they are required to pay; and

   c. Ordering Defendants to engage in a corrective advertising campaign;

6. Awarding damages, as appropriate;

7. Awarding attorneys' fees, costs, and expenses; and

8. Providing such further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Consumer Plaintiffs hereby demand a jury trial of their claims to the extent authorized by

law.

Respectfully Submitted,

HIPSKIND & MCANINCH, LLC

By: /s/ John Hipskind

John T. Hipskind, #6296743
Brady M. McAninch, #6306542
5111 West Main Street
Belleville, Illinois 62226
Phone: 618-641-9189
Fax: 618-551-2642
Attorneys for Plaintiffs