IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

Susan McGann, Mary Lowe, Joseph Lumetta, Steven Kane, Darrius Stewart, Sarah Lamb, Steve Skurat, Kristen MacDonald, and John Gaffigan, individually and on behalf of all others similarly situated,	)	Cause No. 1322-CC00800
	)	Division: 1
	)	**JURY TRIAL DEMANDED**
Plaintiffs,	)	
vs.	)	
Schnuck Markets, Inc., a Missouri corporation,	)	
Defendant.	)	

SECOND AMENDED CLASS ACTION PETITION

COME NOW Plaintiffs Susan McGann, Mary Lowe, Joseph Lumetta, Steven Kane, Darrius Stewart, Sarah Lamb, Steve Skurat, Kristen MacDonald, and John Gaffigan ("Plaintiffs") individually and on behalf of all others similarly situated, and bring this Second Amended Class Action Petition against defendant Schnuck Markets, Inc. ("Defendant" or "Schnucks"), and complain and allege upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Schnucks for its failure to secure and safeguard its customers' personal financial data—including credit and debit card numbers, expiration dates and 3-digit security code information (collectively, "Personal identifying information" or "PII")—and failure to provide clear, conspicuous, and timely notice to Plaintiffs and the other members of the Class that their information had been stolen.

2. On or about March 15, 2013, Schnucks detected that its computer systems had been compromised by one or more individuals, which allowed these individuals to steal Plaintiffs' and Class members' PII—including their credit card information, debit card information, expiration dates and 3-digit security code information—when Plaintiffs and Class members used their credit and debit cards to make purchases from Schnucks (the "Data Breach").

3. Schnucks' security failures enabled the hackers to steal Plaintiffs' and Class members' PII from within Schnucks' computer systems and subsequently make unauthorized purchases on customers' credit cards and otherwise put Plaintiffs' and Class members' financial information at serious and ongoing risk. The hackers might continue to use, or try to use, the information they obtained as a result of Schnucks' inadequate security to exploit and injure Plaintiffs and Class members, even though preventative measures have been taken.

4. The Data Breach was caused and enabled by Schnucks' violation of its obligations to abide by best practices and industry standards concerning the security of its computer and payment processing systems. Schnucks grossly failed to comply with security standards and allowed its customers' PII to be compromised by cutting corners on security measures that could have prevented or mitigated the Data Breach that occurred.

5. Schnucks failed to disclose the extent of the Data Breach, failed to individually notify each of its affected customers of the Data Breach in a timely manner, and failed to take other reasonable steps to clearly and conspicuously inform Plaintiffs and Class members of the nature and extent of the Data Breach. By failing to provide adequate notice, Schnucks prevented Plaintiffs and Class members from protecting themselves from the Data Breach. In fact, many Schnucks customers first learned that their PII had been stolen after being notified of misuse on

their credit and debit cards from their card-issuing financial institutions.

6. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class, assert claims for breach of implied contract, violation of the Missouri Merchandising Practices Act, and invasion of privacy, and seek injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief authorized in equity or by law.

II. JURISDICTION AND VENUE

7. The Court has jurisdiction over the parties and the subject matter of this action.

8. Venue is proper in the City of St. Louis, pursuant to §407.025 RSMo., because many of the acts complained of occurred in the City of St. Louis and because some of the Plaintiffs reside in the City of St. Louis.

III. PARTIES

9. Plaintiff Susan McGann is a resident of the City of St. Louis, Missouri. Plaintiff McGann shopped at the Schnucks store on Hampton Avenue in the City of St. Louis on multiple occasions between December 2012 and March 2013. Plaintiff swiped her debit card through one of that store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of her card information, and had her PII exposed as a result of Schnucks' inadequate security. Schnucks did not provide Plaintiff with timely or effective notification about the Data Breach. Plaintiff viewed her card statement and discovered fraudulent charges on her March 2013 statement, for purchases made in California. Plaintiff contacted her card issuer to report the fraud, and the card issuer canceled her card and issued her a new card. Plaintiff was without use of her card until a replacement card arrived.

10. Plaintiff Mary Lowe is a resident of St. Louis County, Missouri. Plaintiff Lowe shopped at the Schnucks store in Brentwood, Missouri on multiple occasions between December

2012 and March 2013. Plaintiff swiped her debit card and credit card through one of that store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of her card information, and had her PII exposed as a result of Schnucks' inadequate security. Schnucks did not provide Plaintiff with timely or effective notification about the Data Breach. Plaintiff's card issuing institution called her in March 2013 in regard to fraudulent charges on her cards in March 2013, for purchases made in Ohio, California and Tennessee. Plaintiff's card issuer canceled her cards and issued her new cards. Plaintiff was without use of her cards until replacement cards arrived.

11. Plaintiff Joseph Lumetta is a resident of St. Charles County, Missouri. Plaintiff Lumetta shopped at the Schnucks store on Zumbehl in St. Charles County on multiple occasions between December 2012 and March 2013. Plaintiff swiped his debit card through one of that store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of his card information, and had his PII exposed as a result of Schnucks' inadequate security. Schnucks did not provide Plaintiff with timely or effective notification about the Data Breach. Plaintiff discovered that his card was fraudulently used in South Carolina. Plaintiff contacted his card issuer to report the fraud, and the card issuer canceled his card. Plaintiff is without the use of his card until a replacement card arrives.

12. Plaintiff Steve Kane is a resident of the City of St. Louis, Missouri. Plaintiff Kane shopped at the Schnucks store on Hampton Avenue in the City of St. Louis on multiple occasions between December 2012 and March 2013. Plaintiff swiped his debit card through one of that store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of his card information, and had his PII exposed as a result of Schnucks' inadequate security. Schnucks did not provide Plaintiff with timely or effective

notification about the Data Breach. Plaintiff discovered that his card was fraudulently used in Arizona. Plaintiff contacted his card issuer to report the fraud, and the card issuer canceled his card and issued to him a new card. Plaintiff was without use of his card until a replacement card arrived.

13. Plaintiff Darrius Stewart is a resident of the St. Louis County, Missouri. Plaintiff Stewart shopped at the Schnucks store on Watson on multiple occasions between December 2012 and March 2013. Plaintiff swiped his debit card through one of that store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of his card information, and had his PII exposed as a result of Schnucks' inadequate security. Schnucks did not provide Plaintiff with timely or effective notification about the Data Breach. Plaintiff discovered that his card was fraudulently used in Mexico. Plaintiff contacted his card issuer to report the fraud, and the card issuer canceled his card and issued to him a new card. Plaintiff was without use of his card until a replacement card arrived.

14. Plaintiff Sarah Lamb is a resident of the St. Louis County, Missouri. Plaintiff Lamb shopped at the Schnucks stores on Arsenal in the City of St. Louis and at the Brentwood and Webster Groves Schnucks stores on multiple occasions between December 2012 and March 2013. Plaintiff swiped her debit card through those store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of her card information, and had her PII exposed as a result of Schnucks' inadequate security. Schnucks did not provide Plaintiff with timely or effective notification about the Data Breach. Plaintiff discovered that her card was fraudulently used in Florida and Georgia. Plaintiff contacted her card issuer to report the fraud, and the card issuer canceled her card. Plaintiff is without use of her card until a replacement card arrives.

15. Plaintiff Steve Skurat is a resident of the St. Charles County, Missouri. Plaintiff Skurat shopped at the Schnucks store in St. Charles on multiple occasions between December 2012 and March 2013. Plaintiff swiped his debit card through one of that store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of his card information, and had his PII exposed as a result of Schnucks' inadequate security. Schnucks did not provide Plaintiff with timely or effective notification about the Data Breach. Plaintiff discovered that his card was fraudulently used in Louisiana. Plaintiff contacted his card issuer to report the fraud, and the card issuer canceled his card and issued to him a new card. Plaintiff was without use of his card until a replacement card arrived.

16. Plaintiff Kristen MacDonald is a resident of St. Louis County, Missouri. Plaintiff MacDonald shopped at the Schnucks store in Kirkwood on multiple occasions between December 2012 and March 2013. Plaintiff swiped her debit card through those store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of her card information, and had her PII exposed as a result of Schnucks' inadequate security. Schnucks did not provide Plaintiff with timely or effective notification about the Data Breach. Plaintiff discovered that her card was fraudulently used in California. Plaintiff contacted her card issuer to report the fraud, and the card issuer canceled her card. Plaintiff was without the use of her card until a replacement card arrived.

17. Plaintiff John Gaffigan is a resident of the St. Louis County, Missouri. Plaintiff Skurat shopped at the Schnucks store on Butler Hill on multiple occasions between December 2012 and March 2013. Plaintiff swiped his credit card through one of that store's PIN pad terminals and, as a result, entered into an implied contract with Schnucks for the adequate protection of his card information, and had his PII exposed as a result of Schnucks' inadequate

security. Schnucks did not provide Plaintiff with timely or effective notification about the Data Breach. Plaintiff discovered that his card was fraudulently used in Texas. Plaintiff's card issuer canceled his card and issued to him a new card. Plaintiff was without use of his card until a replacement card arrived.

18. Schnuck Markets, Inc. is a Missouri company with its headquarters in St. Louis, Missouri. Schnucks owns and operates supermarkets, some of which contain in-store pharmacies, in Missouri, Illinois, Indiana, Wisconsin, and Iowa. Schnucks operates bakery, deli foods, floral, coffee, meat, pharmacy, fresh produce, cooked seafood, and fuel departments, and also conducts cooking classes.

IV. FACTUAL BACKGROUND

Schnucks' Obligation to Protect Customer Information

19. Schnucks accepts customer payments for purchases through credit and debit cards issued by members of the payment card industry ("PCI"), such as Visa, MasterCard, Discover, and American Express. Each of these card issuers has PCI compliance requirements, which are generally similar to one another.[1]

20. In 2006, Visa, MasterCard, and other PCI members established the Security Standards Council ("PCI SSC"). PCI SSC is an open global forum responsible for the development, management, education, and awareness of PCI Data Security Standards ("PCI DSS") and related standards for increased security of payment processing systems.

21. Per the PCI SSC, "If you are a merchant that accepts payment cards, you are

[1] *See, e.g.,* American Express: www.americanexpress.com/datasecurity; Discover Financial Services: http://www.discovernetwork.com/merchants/fraud-protection; MasterCard Worldwide: http://www.mastercard.com/sdp; Visa Inc: http://www.visa.com/cisp (last visited Apr. 8, 2013).

required to be compliant with the PCI Data Security Standard."[2]

22. At all times relevant to this action, Schnucks was a merchant that accepts payment cards.

23. To adhere to the PCI DSS, a merchant must:

> 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).[3]

24. PCI compliance also requires that a company "install firewalls and forbid using pass codes that come with applications . . . [and] how credit card data should be stored."[4]

25. On information and belief, Schnucks failed to adequately analyze its computer systems that could expose cardholder data and failed to fix vulnerabilities in its computer systems, which allowed the Data Breach to occur.

26. Further, Schnucks admits that it is a "Level 1" merchant—in that it processes more than 6 million card transactions a year—which requires it "to undergo quarterly network scans and an annual audit."[5]

27. It is not publicly known whether Schnucks compiled and submitted remediation

---

[2] *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 Apr. 8, 2013).

[3] *Id.*

[4] Georgina Gustin, *Schnucks Breach Will Likely Cost Millions*, stltoday.com, available at http://m.stltoday.com/STL/db_259737/contentdetail.htm?contentguid=fJPE1FyS&full=true#display (last visited Apr. 8, 2013).

[5] *Id.*

and validation records, or compliance reports to card issuing banks.

28. In addition,

> Under the PCI standards merchants are only allowed to store the data on the front of payment cards—and only if that data is obfuscated. It forbids merchants from storing data found in the magnetic stripes. Information is also required to be encrypted as it travels from point to point in the payment system—from merchant to processor to credit card company to bank—but as [sic] some points it is decrypted as it passes from one to another.[6]

29. Despite these restrictions, Schnucks allowed all of the information contained on the magnetic strips on the backs of Plaintiffs' and Class members' credit and debit cards in its possession, custody, and control to be compromised.

Data Breaches Lead to Identity Theft

30. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[7] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

31. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money and patience to

---

[6] *Id.*

[7] *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 Apr. 8, 2013).

resolve.[8] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[9]

32. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

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

33. Plaintiffs' and Class members' credit and debit card information that was stolen in the Data Breach at issue in this action is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[10] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers and other PII directly on various Internet websites, making the information publicly available.

34. In fact, "[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud."[11]

---

[8] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at https://www.cboprf.com/What%20To%20Do%20If%20Your%20Identity%20Is%20Stolen.pdf (last visited Apr. 8, 2013).

[9] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[10] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. *See* 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).

[11] *One in Four that Receive Data Breach Letters Affected By Identity Theft*, available at http://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/ (last visited Apr. 8, 2013).

The Schnucks Data Breach

35. On or about March 15, 2013, Schnucks discovered that its computer systems had been compromised by one or more individuals, which allowed these individuals to steal Plaintiffs' and Class members' PII when Plaintiff and Class members used their credit and debit cards to make purchases from Schnucks.

36. Despite knowing the risk to consumers as a result of this breach of its systems, Schnucks knowingly withheld the fact from Plaintiff and Class members that the Data Breach had occurred and that their PII had been compromised.

37. On March 30, 2013—two weeks after Schnucks learned of the Data Breach—Schnucks issued a press release stating that its computer systems had been compromised, and that it had "'found and contained' the issue behind the reports of unauthorized access to payment card information at Schnucks, and it has taken comprehensive measures designed to block any further access."[12]

38. Schnucks revealed that malicious computer code had been planted into its computer systems that captured the magnetic strip data located on the back of credit and debit cards.[13]

39. Schnucks does not know how long its computer systems have been compromised; Schnucks has reported that it does not know how many customers were affected by the Data Breach and insists that its customer database has been secured.[14]

---

[12] *Schnucks Announces Credit Card Issue Found and Contained*, http://www.schnucks.com/pressreleases/pressrelease.asp?id=214 (last visited Apr. 8, 2013).

[13] *Id.*

[14] *Id.*

40. Schnucks further acknowledged that "even though we have contained the attack, any card that was already accessed could still experience fraud,"[15] meaning that Plaintiff and Class members are at a continuing risk of identity theft and identity fraud.

41. According to Chesterfield police spokesman Officer Mike Ryffel, "We have had an increase in fraud reports these past few weeks . . . . We believe the increase is due to the Schnucks security breach."[16]

42. On information and belief, at the time of the Data Breach, Schnucks was not in compliance with PCI requirements or card issuer requirements for the protection of its computer systems.

43. Schnucks' failure to comply with mandated PCI requirements and card issuer requirements for the protection of its computer systems provided Schnucks 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 Schnucks' own customers—including Plaintiff and Class members here—who have been subject to the Data Breach or otherwise have had their financial information placed at serious and ongoing risk.

44. Schnucks allowed widespread and systematic theft of Plaintiffs' and Class members' PII. Schnucks' conduct did not meet the standards of commercially reasonable steps that should be taken to protect Plaintiffs' and Class members' PII. Despite being obligated to do so, Schnucks failed to employ appropriate technical, administrative, or physical procedures to protect Plaintiffs' and Class members' PII from unauthorized capture, dissemination, or misuse,

---

[15] *Id.*

[16] *Police Suspect More Schnucks Fraud Cases Have Hit Residents*, ChesterfieldPatch, available at http://chesterfield.patch.com/articles/police-suspect-more-schnucks-fraud-cases-have-hit-residents (last visited Apr. 8, 2013).

thereby making Plaintiff and Class members easy targets for theft and misuse of their financial information, including in the manner undertaken by the hackers here.

Schnucks Fails to Provide Sufficient Notice of the Data Breach to Plaintiff and Class Members

45. Despite first learning of the Data Breach on or about March 15, 2013, Schnucks did not inform the public of the Data Breach until March 30, 2013—two weeks later—via the issuance of a press release.

46. No known individual notification to Plaintiff and Class members of the Data Breach has occurred.

47. Although Schnucks' press release contains language designed to reassure the reader that customers can make transactions securely with Schnucks,[17] Schnucks does not acknowledge its failure to implement proper security measures *prior* to the breach—when it actually mattered.

48. Rather than take responsibility for its security failures that resulted in the Data Breach, Schnucks has placed the burden on aggrieved customers like Plaintiff and the other members of the Class, either to self-monitor their accounts and credit reports for years to come, or to spend time and money on fraud alerts or credit-report security freezes.

49. Plaintiffs and Class members are subject to continuing damage from having their PII compromised because of Schnucks' inadequate security. Plaintiffs and Class members were and are entitled to clear, conspicuous, and prompt notification about the Data Breach to help them mitigate the harm and avoid additional instances of fraud as alleged herein.

[17] *Id.*

The Monetary Value of Privacy Protections and PII

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

> 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.[18]

51. 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.[19]

52. 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.[20]

53. Recognizing the high value that 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 that they share

---

[18] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm (last visited Apr. 8, 2013).

[19] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, available at http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Apr. 8, 2013).

[20] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), available at http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Apr. 8, 2013).

and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from the surrender of their PII.[21] This business has created a new market for the sale and purchase of this valuable data.[22]

54. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on 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."[23]

55. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use—two concerns at issue here—they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[24]

56. The value of Plaintiffs' and Class members' PII on the black market is substantial—credit card numbers range in cost from $1.50 to $90 per card number.[25] By way of the Data Breach, Schnucks has deprived Plaintiff and Class members of the substantial value of

---

[21] 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 Apr. 8, 2013).

[22] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

[23] Il-Horn Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (emphasis added) (last visited Apr. 8, 2013); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) Information Systems Research 254, 254 (June 2011).

[24] *Id.*

[25] *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 Apr. 8, 2013); Office of the National Counterintelligence Executive, *How Much Do You Cost on the Black Market*, available at http://www.ncix.gov/issues/cyber/identity_theft.php (last visited Apr. 8 2013).

their PII, to which they are entitled.

57. Given these facts, any company that transacts business with consumers and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Damages Sustained By Plaintiff and Class Members

58. A portion of the services purchased from Schnucks by Plaintiffs and Class members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiffs and Class members were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and Class members incurred actual monetary damages in that they overpaid for the products purchased from Schnucks.

59. Plaintiffs and other members of the Class have suffered additional injury and damages, including, but not limited to: (i) the untimely and/or inadequate notification of the Data Breach, which has placed Plaintiffs and Class members at an increased risk of identity theft and/or identity fraud; (ii) improper disclosure of their PII; (iii) loss of and invasion of privacy, and all damages relating thereto that are recoverable at law; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; (vii) anxiety and emotional distress; and (viii) deprivation of the value of their PII, for which there is a well-established national and international market—for which they are entitled to compensation.

60. Plaintiffs and Class members suffered additional damages based on the opportunity cost and value of time that Plaintiffs and Class members have been forced to expend

to monitor their financial and bank accounts as a result of the Data Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

61. Schnucks is instructing customers who swiped their cards at any of the Schnucks stores to take certain steps. Credit and debit card users should review their accounts for unauthorized transactions and notify their banks immediately if they discover any unauthorized purchases or cash advances.

62. Debit card users will now be required to take the time to change their PIN numbers on their debit cards, and both credit and debit card users will have to closely review and monitor their accounts for unauthorized activity. Plaintiffs and Class members now face a greater risk of identity theft.

V. CLASS ALLEGATIONS

63. This action is brought and may be properly maintained as a class action pursuant to Mo. Sup. Ct. R. 52.08, on behalf of a Class defined as follows:

> All persons who made an authorized in-store purchase using a credit or debit card at a Schnucks store between December 9, 2012 through and including March 30, 2013 (the "Class").
>
> Excluded from the Class are: (i) Schnucks and its officers and directors, (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 Breach or who pleads *nolo contendere* to any such charge.

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

65. The members of the Class are so numerous that joinder of the Class members would be impracticable. On information and belief, Class members number in the thousands.

66. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Schnucks failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class members' PII;

b. Whether Schnucks properly implemented its purported security measures to protect Plaintiffs' and Class members' PII from unauthorized capture, dissemination, and misuse;

c. Whether Schnucks took reasonable measures to determine the extent of the Data Breach after it first learned of same;

d. Whether Schnucks' delay in informing Plaintiff and Class members of the Data Breach was unreasonable;

e. Whether Schnucks' method of informing Plaintiff and Class members of the Data Breach (and its description of the breach and potential exposure to damages as a result of same) was unreasonable;

f. Whether Schnucks' conduct violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010, *et seq.*;

g. Whether Schnucks' conduct constitutes breach of an implied contract;

h. Whether Schnucks willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' PII;

i. Whether Schnucks was negligent in failing to properly secure and protect its PIN pads and Plaintiffs' and Class members' PII;

j. Whether by publicly disclosing Plaintiffs' and Class members' PII without authorization, Schnucks invaded Plaintiffs' and Class members' privacy;

k. Whether Schnucks concealed the breach from Plaintiff and Class members; and

l. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

67. Schnucks engaged in a common course of conduct giving rise to the legal rights

sought to be enforced by 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.

68. Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Schnucks' uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Schnucks that are unique to Plaintiffs.

69. Plaintiffs are adequate Class representatives because they will fairly represent the interests of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting consumer class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Class they represent, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse or antagonistic to those of the Class.

70. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The vast majority of damages suffered individually by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Schnucks, so it would be impracticable for Class members to individually seek redress for Schnucks' wrongful conduct. In the event any Class Member chooses to pursue their individual case, they can opt out of the class action. Historically, opt outs do not present a burden on the judicial system, as would the multitude of filings if each class member would be forced to pursue an individual case. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far

fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS

COUNT I
Breach of Implied Contract

71. Plaintiffs incorporate paragraphs 1–72, as if fully set forth herein.

72. Schnucks' customers who intended to make in-store purchases with debit or credit cards were required to provide their card's magnetic strip data and PINs (for debit cards)—their PII—for payment verification.

73. In providing such financial data, Plaintiffs and the other members of the Class entered into an implied contract with Schnucks, whereby Schnucks became obligated to reasonably safeguard Plaintiffs' and the other Class members' PII.

74. Under the implied contract, Schnucks was obligated to not only safeguard the PII, but also to provide Plaintiffs and Class members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

75. Schnucks breached the implied contract with Plaintiffs and the other members of the Class by failing to take reasonable measures to safeguard their PII.

76. Schnucks also breached its implied contract with Plaintiffs and the other Class members by failing to provide prompt, adequate notice of the Data Breach and unauthorized access of their PII by hackers.

77. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them

by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and (vii) deprivation of the value of their PII, for which there is a well-established national and international market—for which they are entitled to compensation. At the very least, Plaintiffs and Class members are entitled to nominal damages.

COUNT II
Violation of the
Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010, *et seq.*, ("MMPA")

78. Plaintiffs incorporate paragraphs 1–72, as if fully set forth herein.

79. Plaintiffs and Class members are consumers who purchased goods and services from Schnucks primarily for personal, family or household purposes.

80. Plaintiffs and the other members of the Class were subjected to Schnucks' unfair conduct in failing to properly implement adequate, commercially reasonable security measures to protect their PII while shopping at Schnucks.

81. Schnucks intended for Plaintiffs and the other members of the Class to rely on Schnucks to protect the PII furnished to it in connection with their credit and debit card transactions in such a manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

82. Schnucks instead handled Plaintiffs' and the other Class members' PII in such a manner that it was compromised.

83. Schnucks either willfully ignored its obligations to PCI members in failing to follow industry best practices concerning data theft, or was negligent in preventing such data theft from occurring when it allowed the Data Breach to occur.

84. It was foreseeable that Schnucks' willful indifference or negligent course of

conduct in handling Plaintiffs' and Class members' PII would put that information at risk of compromise by data thieves.

85. Schnucks benefited from not taking preventative measures that would have prevented the data from being compromised, because Schnucks saved on the cost of those security measures.

86. Schnucks omitted these material facts from Plaintiffs and Class members regarding the inadequate security of its computer systems.

87. Schnucks' omissions were intended to induce Plaintiffs' and the other Class members' reliance on the fact that their PII was secure and protected when using credit and debit cards to shop at Schnucks.

88. Section 407.020 of the Missouri Merchandising Practices Act provides in pertinent part:

> The act, use of employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce . . . is declared to be an unlawful practice.

89. The acts and misconduct of Schnucks as alleged above violated the Missouri Merchandising Practices Act by, among other things, constituting a deceptive and unfair practice.

90. Schnucks' conduct as alleged herein occurred in the course of trade or commerce and Plaintiffs' and Class members' PII was provided to Schnucks primarily for personal, family or household purposes.

91. Schnucks' unauthorized disclosure of Plaintiffs' and other Class members' PII constitutes an unfair practice. Further, Schnucks' failure to properly give timely and sufficient notice of the breach of the security of its computer systems further constitutes an unfair practice.

92. Plaintiffs and other members of the Class have suffered an ascertainable loss of money or property, real or personal, as a result of the use or employment by Defendant of a method, act or practice declared unlawful by §407.020 RSMo.

93. Plaintiffs and the other Class members suffered ascertainable loss as a result of Schnucks' unfair trade practices, including but not limited to: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and (vii) deprivation of the value of their PII, for which there is a well-established national and international market—for which they are entitled to compensation. At the very least, Plaintiffs and Class members are entitled to nominal damages.

94. Plaintiffs' and Class members' injuries were proximately caused by Schnucks' unfair practices, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

95. Pursuant to Section 407.025.1 RSMo., the Court may award attorney's fees to Plaintiffs and the Class.

COUNT III
Invasion of Privacy By Public Disclosure of Private Facts

96. The preceding factual statements and allegations are incorporated herein by reference.

97. Plaintiffs' and Class members' PII was (and continues to be) private information.

98. Schnucks' failure to secure and protect Plaintiffs' and Class members' PII directly resulted in the public disclosure of such private information.

99. Dissemination of Plaintiffs' and Class members' PII is not of a legitimate public concern; publicity of their PII would be, is, and will continue to be offensive to Plaintiffs, Class members, and other reasonable people.

100. Plaintiffs and Class members were (and continue to be) damaged as a direct and/or proximate result of Schnucks' invasion of their privacy by publicly disclosing their private facts (*i.e.*, their PII) in the form of, *inter alia*: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; (vii) deprivation of the value of their PII, for which there is a well-established national and international market; and (viii) anxiety and emotional distress—for which they are entitled to compensation. At the very least, Plaintiffs and the Class members are entitled to nominal damages.

101. Schnucks' wrongful actions and/or inaction (as described above) constituted (and continue to constitute) an invasion of Plaintiffs' and Class members' privacy by publicly disclosing their private facts (*i.e.*, their PII).

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this Second Amended Petition so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Second Amended Petition, respectfully request that the Court enter judgment in their favor and against Schnuck Markets, Inc., as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives and appointing Plaintiffs' counsel as Lead Counsel for the Class;

B. declaring that Schnucks breached its implied contract with Plaintiffs and Class members;

C. declaring that Schnucks has violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010, *et seq.*;

D. declaring that Schnucks has invaded Plaintiffs' and Class members' privacy;

E. Ordering Schnucks to pay actual damages to Plaintiff and the other members of the Class;

F. Ordering Schnucks to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

G. Ordering Schnucks to pay statutory damages, as provided by the Missouri Merchandising Practices Act;

H. Ordering Schnucks to disseminate constitutionally required notice;

I. Ordering Schnucks to pay attorneys' fees and litigation costs to Plaintiffs;

J. Ordering Schnucks to pay both pre- and post-judgment interest on any amounts awarded; and

K. Ordering such other and further relief as may be just and proper.

Respectfully submitted,

/s/ John S. Steward
John S. Steward, #45932
STEWARD LAW FIRM, LLC
1717 Park Avenue
St. Louis, Missouri 63104
314-571-7134
314-594-5950 fax
Glaw123@aol.com

Joseph V. Neill, #28472
ATTORNEY AT LAW
5201 Hampton Avenue
St. Louis, Missouri 63109
314-353-1001
314-353-0181 fax
Neill5300@aol.com

Geoffrey S. Meyerkord, #46556
MEYERKORD & MEYERKORD, LLC
1717 Park Avenue
St. Louis, Missouri 63104-2941
314-436-9958
314-446-4700 fax
gsm@meyerkordlaw.com

Attorneys for Plaintiffs

OF COUNSEL:
Ben Barnow (*pro hac vice pending*)
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
312-621-2000
312-641-5504 fax
b.barnow@barnowlaw.com

Certificate of Service

The undersigned hereby certifies a true and correct copy of the foregoing was served via filing with the Court's e-filing service, on this 1st day of October, 2013, to:

Kevin Hormuth
Greensfelder, Hemker & Gale, P.C.
2000 Equitable Bldg
10 S Broadway
St. Louis, MO 63102

/s/ John Steward