**UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF ILLINOIS**
**EAST ST. LOUIS DIVISION**

| | | |
|---|---|---|
| **COMMUNITY BANK OF TRENTON, UNIVERSITY OF ILLINOIS EMPLOYEES CREDIT UNION, FIRST FEDERAL SAVINGS BANK OF CHAMPAIGN-URBANA, and SOUTHPOINTE CREDIT UNION, individually and on behalf of all similarly situated payment card issuers,** | § | **CIVIL ACTION NO. 3:15-cv-01125-MJR** |
| | § | **JURY TRIAL DEMANDED** |
| **PLAINTIFFS** | § | |
| | § | **EQUITABLE RELIEF IS SOUGHT** |
| **v.** | § | |
| **SCHNUCK MARKETS, INC.,** | § | |
| **DEFENDANT** | § | |

# FIRST AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND

Richard L. Coffman
**THE COFFMAN LAW FIRM**
First City Building
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

John J. Driscoll
Christopher J. Quinn
**THE DRISCOLL FIRM, PC**
211 N. Broadway, 40th Floor
St. Louis, MO 63102
Telephone: (314) 932-3232
Email: john@thedriscollfirm.com
Email: chris@thedriscollfirm.com

G. Robert Blakey
Professor of Law Emeritus
Notre Dame Law School*
7002 East San Miguel Ave.
Paradise Valley, AZ 85253
Telephone: (574) 514-8220
Email: blakey.1@nd.edu
* Noted for identification only

Mitchell A. Toups
**WELLER, GREEN TOUPS & TERRELL, LLP**
2615 Calder Ave., Suite 400
Beaumont, TX 77702
Telephone: (409) 838□0101
Facsimile: (409) 838□6780
Email: matoups@wgttlaw.com

**ATTORNEYS FOR PLAINTIFFS AND THE PUTATIVE CLASS**

**TABLE OF CONTENTS**

Plaintiffs Community Bank of Trenton, University of Illinois Employees Credit Union (now known as University of Illinois Community Credit Union), First Federal Savings Bank of Champaign-Urbana, and Southpointe Credit Union (now known as Members 1st Credit Union) (collectively, "Plaintiffs"), individually and on behalf of all similarly situated financial institutions (the "Class Members"), and based upon known facts and upon information and belief, respectfully complain of the actions of Defendant Schnuck Markets, Inc. ("Schnucks"):

## NATURE OF THE CASE

**1.** This is a data breach case. It is virtually identical to the data breach cases involving compromised debit cards and credit cards (together, "payment cards") brought by large, sophisticated financial institutions against retailers, such as Target and Home Depot, for failing to safeguard and protect confidential payment card information.[1] The courts in both *Target* and *Home Depot* declined to dismiss all of the financial institution plaintiffs' claims—several of which are asserted here—and, in fact, Target settled the financial institution plaintiffs' claims for $39.35 million.[2]

**2.** The sophistication level of the financial institution plaintiffs in *Target* and *Home Depot* was not in issue. Rather, the issue was whether Target and Home Depot owed the financial institution plaintiffs a duty to safeguard and protect confidential payment card information in their possession, custody, and control, whether Target and Home Depot violated such duty, and, if so, the amount of damages incurred by the financial institution plaintiffs as a

---

[1] *See, e.g., In re Target Corporation Customer Data Security Breach Litigation*; MDL No. 2522 (D. Minn.) (financial institution case); *In re The Home Depot, Inc. Customer Data Breach Litigation*; MDL No. 2583 (N.D. Ga.) (financial institution case).

[2] *See* TARGET DATA BREACH SETTLEMENT WEBSITE RELATING TO FINANCIAL INSTITUTIONS, https://www.targetbanksettlement.com/FrequentlyAskedQuestions#q4 (FAQ No. 4) (last visited Oct. 3, 2016).

direct or proximate result of the respective Target and Home Depot data breaches.[3] Both courts held that the financial institution plaintiffs plausibly pled such a duty. *Id*.

**3.** Plaintiffs are small town banks, savings banks, and credit unions. Schnucks, a member of the Forbes 2016 List of America's Largest Private Companies,[4] is one of the largest privately held supermarket chains in the United States, with annual revenue of $2.7 billion.

**4.** Plaintiffs and Class Members are similarly situated financial institutions that issued approximately 2.4 million payment cards compromised by a data breach of Schnucks' internal computer systems (the "Schnucks Data Breach" or "Data Breach" or "Breach"), from December 2012 through March 30, 2013. The Data Breach resulted from Schnucks' failure to safeguard and protect the confidential payment card information of the payment cards issued by Plaintiffs and Class Members. Schnucks had a duty to Plaintiffs and Class Members to safeguard and protect such confidential information. Schnucks failed to do so.

**5.** As part and parcel of the Schnucks Data Breach, hackers targeted specific vulnerabilities in Schnucks' computer systems, hijacking unencrypted and improperly protected confidential payment card information from Schnucks' "processing environment" within its internal computer systems while electronic payment card transactions awaited approval. The hackers had an open door into Schnucks' computer systems. They waltzed through the door, installed malware in Schnucks' "processing environment," and spent months harvesting confidential payment card information and other customer data from approximately 79 of the 100 Schnucks retail locations in Missouri, Illinois, Indiana, Iowa, and Wisconsin. The malware

---

[3] *See In re Target Corporation Customer Data Security Breach Litig.*, 64 F.Supp.3d 1304 (D. Minn. 2014) (financial institution case); *In re The Home Depot, Inc. Customer Data Breach Litig.*, MDL No. 1:14-md-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016) (financial institution case).

[4] *See* FORBES 2016 LIST OF AMERICA'S LARGEST PRIVATE COMPANIES, http://www.forbes.com/largest-private-companies/#/tab:rank_page:17 (last visited Oct. 3, 2016).

"skimmed" or "scraped" payment card numbers and expiration dates (and possibly more information and data) from electronic payment card transactions, stored the payment card information in a hijacked server within Schnucks' internal computer systems, and later transmitted the payment card information to the hackers via the Internet.

**6.** The wrongfully disclosed and compromised confidential payment card information was then sold by the hackers (or their fraudster customers) on illicit black market Internet websites as "dumps" to international card counterfeiters and other fraudsters. The fraudsters then used the purloined confidential payment card information to create counterfeit payment cards used to make fraudulent purchases and withdraw cash from the financial accounts of unsuspecting victims through ATMs. Confirmed fraud involving the wrongfully disclosed and compromised confidential payment card information was detected by multiple payment card processing companies well before March 30, 2013, the date Schnucks first reported the Data Breach to the general public.

**7.** Schnucks knew that Plaintiffs and Class Members are part of the Visa and MasterCard Networks and rely on merchants like Schnucks that accept Visa and MasterCard payment cards to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems across their computer systems. Schnucks also knew that its below-described wrongful actions, inaction, and omissions were unlawful, and would cause Plaintiffs and Class Members to suffer damages and other actual injury and harm as a direct result of the Data Breach.

**8.** The Schnucks Data Breach should (and could) have, been prevented if Schnucks had implemented the appropriate customer data security policies, procedures, protocols, and hardware and software systems across its computer systems, and complied with the Payment

Card Industry Data Security Standards ("PCI DSS"),[5] the Visa Operating Regulations and MasterCard Rules (together, the "Card Brand Rules"), and Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.[6]

**9.** Schnucks' wrongful actions, inaction, and omissions, and the resulting Data Breach constitute negligence/gross negligence, negligence *per se*, breach of implied contract, breach of contract to which Plaintiffs and Class Members are third-party beneficiaries, breach of the Illinois Consumer Fraud and Deceptive Business Practices Act, and unjust enrichment/assumpsit.

**10.** As a direct and proximate result of Schnucks' wrongful conduct, Plaintiffs and Class Members have incurred (and will continue to incur) damages to their business and property, and other actual injury and harm in the form of, *inter alia*, (i) the time and out-of-pocket expenses to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest and transaction fees due to reduced payment card usage.

---

[5] *See* PCI SECURITY STANDARDS COUNCIL DOCUMENT LIBRARY, https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited Oct. 3, 2016).

[6] Schnucks' failure to implement, monitor, and maintain the proper customer data security policies, procedures, protocols, and hardware and software systems constitutes unlawful, unfair, and deceptive acts or practices in, or affecting, commerce prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45(a). *See, e.g.*, Ryan T. Bergsieker, Richard H. Cunningham, and Lindsey Young, *The Federal Trade Commission's Enforcement of Data Security Standards*, 44 THE COLORADO LAWYER 39-43 (June 2015); *In re The Home Depot, Inc. Customer Data Breach Litig.*, 2016 WL 2897520, at *4 (Financial institution plaintiffs' "Consolidated Class Action Complaint here adequately pleads a violation of Section 5 of the FTC Act, that the Plaintiffs are within the class of persons intended to be protected by the statute, and that the harm suffered is the kind the statute meant to protect.").

**11.** Plaintiffs, for themselves and Class Members, seek to recover their (i) above-described damages, (ii) punitive damages, (iii) equitable relief, (iv) declaratory relief, (v) injunctive relief requiring Schnucks to, *inter alia*, implement proper customer data protection policies, procedures, protocols, hardware and software systems and discontinue its above-described wrongful conduct, (vi) pre- and post-judgment interest, (vii) attorneys' fees, litigation expenses, court costs, and (viii) such other relief the Court deems just and proper.

## JURISDICTION AND VENUE

**12.** This Court has subject matter jurisdiction over Plaintiffs' claims under (i) 28 U.S.C. § 1332(d) (CAFA), because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state diverse from the citizenship of Schnucks, and (c) the matter in controversy exceeds $5,000,000 USD, exclusive of interest and costs; and (ii) 28 U.S.C. § 1367 (supplemental jurisdiction). This Court also has *in personam* jurisdiction over Schnucks because at all relevant times, Schnucks resided, was found, and conducted business in the East St. Louis Division of the Southern District of Illinois, and Plaintiff Community Bank of Trenton is located in the East St. Louis Division of the Southern District of Illinois. *Community Bank of Trenton v. Schnuck Markets, Inc.*, No. 15-cv-01125-MJR, 2016 WL 5409014, at *1 (S.D. Ill. Sept. 28, 2016). Schnucks does not contest jurisdiction. *Id*.

**13.** At all relevant times, Schnucks resided, was found, and conducted business in the East St. Louis Division of the Southern District of Illinois, and Plaintiff Community Bank of Trenton is located in the East St. Louis Division of the Southern District of Illinois. Accordingly, venue is proper in this Court under 28 U.S.C § 1391(a). *Community Bank of Trenton*, 2016 WL 5409014, at *1. Nor does Schnucks contest venue. *Id*.

## PARTIES

**14.** Plaintiff Community Bank of Trenton ("CBT") is a small Illinois bank located in Trenton, Illinois (population 2667).[7] CBT has one location and approximately 15 employees. CBT canceled and re-issued more than 300 Visa CheckCard debit cards compromised by the Schnucks Data Breach. As a direct and proximate result of Schnucks' above-described wrongful conduct and the resulting Data Breach, CBT (to date) has incurred damages to its business and property, and other actual injury and harm in the form of, *inter alia*, (i) over $4,000 in time and out-of-pocket expenses to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) hundreds of dollars in fraudulent charges and/or "chargeback" fees related to fraudulent charges made on the compromised payment cards reimbursed to customers, and (iii) lost transaction fees due to reduced payment card usage in an amount to be determined by the trier of fact.

**15.** Plaintiff University of Illinois Employees Credit Union ("UIECU") (now known as University of Illinois Community Credit Union) is a small Illinois credit union located in Champaign, Illinois (population 86,096).[8] UIECU has three locations and 105 employees. UIECU canceled and re-issued 5369 payment cards compromised by the Schnucks Data Breach. As a direct and proximate result of Schnucks' above-described wrongful conduct and the resulting Data Breach, UIECU (to date) has incurred damages to its business and property, and other actual injury and harm in the form of, *inter alia*, (i) over $45,000 of time and out-of-pocket

---

[7] Estimated as of July 1, 2015. *See* UNITED STATES CENSUS BUREAU, ANNUAL ESTIMATES OF THE RESIDENT POPULATION: APRIL 1, 2010 TO JULY 1, 2015, http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk (last visited Oct. 3, 2106) ("July 2015 CENSUS BUREAU ESTIMATES").

[8] *Id*.

expenses to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) over $195,000 of fraudulent charges and/or "chargeback" fees related to fraudulent charges made on the compromised payment cards reimbursed to customers, and (iii) lost interest and transaction fees due to reduced payment card usage in an amount to be determined by the trier of fact.

**16.** Plaintiff First Federal Savings Bank of Champaign-Urbana ("FFSB") is a small, federally-chartered savings bank located in Champaign, Illinois (population 86,096).[9] FFSB has two locations and 60 employees. FFSB canceled and re-issued 1203 payment cards compromised by the Schnucks Data Breach. As a direct and proximate result of Schnucks' above-described wrongful conduct and the resulting Data Breach, FFSB (to date) has incurred damages to its business and property, and other actual injury and harm in the form of, *inter alia*, (i) approximately $20,000 of employee time and out-of-pocket expenses to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) over $18,000 of fraudulent charges and/or "chargeback" fees related to fraudulent charges made on the compromised payment cards reimbursed to customers, and (iii) lost interest and transaction fees due to reduced payment card usage in an amount to be determined by the trier of fact.

**17.** Plaintiff Southpointe Credit Union ("SPCU") (now known as Members 1st Credit Union) is a small Missouri credit union located in a far southern suburb of St. Louis, Missouri, with a second location in Festus Missouri (population 12,065).[10] SPCU has two locations and 14 employees (8 at the time of the Data Breach). SPCU canceled and re-issued 368 payment cards

[9] *Id.*

[10] *Id.*

compromised by the Schnucks Data Breach. As a direct and proximate result of Schnucks' above-described wrongful conduct and the resulting Data Breach, SPCU (to date) has incurred damages to its business and property, and other actual injury and harm in the form of, *inter alia*, (i) over $3200 of time and out-of-pocket expenses to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) over $8500 of fraudulent charges and/or "chargeback" fees related to fraudulent charges made on the compromised payment cards reimbursed to customers, and (iii) lost interest and transaction fees due to reduced payment card usage in an amount to be determined by the trier of fact.

**18.** Defendant Schnucks is a Missouri corporation headquartered in St. Louis, Missouri. With nearly 15,000 employees, Schnucks owns and operates 99 retail supermarkets in Missouri, Indiana, Wisconsin, Iowa, and Illinois—including the Southern District of Illinois. Schnucks is No. 48 on the 2016 Supermarket News Top 75 U.S. and Canadian Food Retailers and Wholesalers. With annual revenue of $2.7 billion, Schnucks is one of the largest privately held retail grocery chains in the United States. The Data Breach, and Schnucks' wrongful actions, inaction, and omissions leading to the Breach (as described in detail below), occurred in Missouri. Schnucks has been served with Summons and appeared in this lawsuit.

## FACTS

**19.** Consumers suffer substantial damages when a merchant's failure to properly secure its electronic payment card processing systems results in a security breach.[11] But financial institution payment card issuers, such as Plaintiffs, bear the brunt of direct economic losses.[12]

---

[11] *See, generally, Remijas v. Neiman Marcus Grp., LLC,* 794 F.3d 688, 692-93, 694 (7th Cir. 2015) (discussing consumers' damages).

[12] *Banks Bear Cost of Store Data Breaches,* available at http://www.semissourian.com/story/2045315.html (last visited October 5, 2016); *In a Cyber Breach, Who Pays, Banks or*

**20.** That is because financial institutions are required to reimburse their customers for charges made by fraudsters who purchase goods using customers' compromised payment card information,[13] cannot recoup some or all of the reimbursed fraudulent charges, and must pay "chargeback" and other fees in connection with the disputed charges. Financial institutions also incur significant costs associated with cancelling and reissuing thousands (if not tens of thousands or more) of compromised payment cards – at a typical average cost of more than $10 per card – which they must do in order to avoid future fraud losses.[14]

**21.** As this case and other cases demonstrate, financial institutions necessarily rely on merchants to honor their obligations under the PCI DSS, Card Brand Rules, Section 5 of the FTC Act, and state data breach notification statutes, to (i) properly secure their payment card processing systems and (ii) immediately report any payment card data security breach so that the issuing financial institutions may take appropriate steps to minimize their fraud losses, including declining potentially fraudulent transactions, canceling and re-issuing potentially compromised payment cards, and warning their customers when a merchant—like Schnucks here—declines to timely do so.

**22.** As explained below, Schnucks breached its obligations before, during, and after the Data Breach, thereby causing Plaintiffs and Class Members to suffer losses in the tens of millions of dollars. And while Schnucks has compensated consumers damaged by its wrongful

---

*Retailers?,* http://www.wsj.com/articles/SB10001424052702303819704579316861842957106 (last visited October 5, 2016).

[13] *See, e.g.,* 15 U.S.C. § 1643 (limiting cardholder liability for unauthorized use of a credit card); 12 C.F.R. § 205.6 (limiting liability of debit card holders for unauthorized transactions).

[14] *See* n.12, *supra.* Thus, the cost to cancel and re-issue payment cards compromised by the Data Breach alone exceeds $20 million. This is in addition to fraudulent charges made on the compromised payment cards that were reimbursed by Plaintiffs and Class Members, and other Data Breach-related damages.

acts and omissions,[15] it has refused to reimburse the injured financial institutions, many of which are small community banks, savings banks, and credit unions, with revenues that pale in comparison with that of Schnucks.[16]

**23.** If merchants, like Schnucks, that knowingly ignore their payment card data security and data breach reporting obligations are permitted to pass the cost of their wrongful conduct to issuing financial institutions, they have no reason to act otherwise.[17] One example: although the Data Breach here resulted from the theft of "track data" stored on the magnetic strips of customers' cards, as discussed below, Schnucks' customers do not – to this day – have the option to pay for goods using EMV "chip cards," which provide "much greater security"[18] than magnetic strip cards.

## I. Payment Card Transactions on the Visa and MasterCard Networks.

**24.** Schnucks derives the majority of its revenue from payment card purchases. Issuing financial institutions, such as Plaintiffs and Class Members, in turn, earn interchange or "swipe" fees when customers use debit cards, and interest when customers use credit cards.

**25.** When a customer makes a payment card purchase at a Schnucks supermarket, Schnucks collects confidential payment card information and other customer data stored on the

---

[15] *See Schnucks Agrees to Proposed Settlement Over Data Breach,* http://www.stltoday.com/business/local/schnucks-agrees-to-proposed-settlement-over-data-breach/article_5b3fcc41-5b97-5063-9def-a46e144aad85.html (last accessed October 5, 2016).

[16] *Why Work at Schnucks,* https://www.schnucks.com/Careers/Why-Work-at-Schnucks/ (last visited October 5, 2016) ("Schnucks is one of the top 100 privately owned companies and one of the top 10 privately owned supermarket chains nationwide" with "100 stores in Missouri, Illinois, Indiana, Iowa and Wisconsin" and "annual sales in excess of $2.1 billion.")

[17] *See Banks Bear Cost of Store Data Breaches,* available at http://www.semissourian.com /story/2045315.html (last visited October 5, 2016).

[18] *Chip Cards Gain Steam, Forcing Hackers to Get Crafty,* http://www.cnbc.com /2016/09/30/chip-cards-gain-steam-forcing-hackers-to-get-crafty.html (last visited October 5, 2016).

magnetic strip of the payment card, including the cardholder's name, account number, expiration date, CVV code (a numeric security code), and in the case of a debit card, the customer's PIN number (collectively, "track data"). Schnucks stores this information in its computer systems while electronically transmitting the information to third parties in the Visa and MasterCard Networks to process the electronic transaction for payment. Schnucks also collects and stores other consumer data, including mailing addresses, phone numbers, and email addresses.

**26.** Track data is highly valuable on the black market because once in the hands of fraudsters, it can be used to create new payment cards and make fraudulent purchases.

**27.** A typical payment card transaction made on the Visa and MasterCard Networks involves multiple electronic transactions handled by several different parties. In basic terms, when a payment card purchase is made, the merchant seeks authorization from the issuing financial institution (or, sometimes, the issuing financial institution's card processing vendor), which verifies that the payment card is valid, not reported as lost, stolen or otherwise compromised, and the account has funds or credit sufficient to cover the transaction amount.[19] If the transaction is approved, the issuing financial institution posts the charge to the consumer's payment card account, and the merchant receives payment over the network. If the transaction is declined, no funds are transferred.

## II. The Data Breach happened because Schnucks knowingly failed to comply with the PCI DSS, the Card Brand Rules, and Section 5 of the FTC Act.

**28.** By accepting credit card and debit cards for payment, Schnucks is legally and contractually obligated to abide by best practices and industry standards concerning the security

[19] In reality, the transaction is somewhat more complex and involves intermediary institutions, including the merchant's acquiring bank (a financial institution that contracts with the merchant to process its payment card transactions), a payment card transaction processor (an entity retained by the acquiring bank to actually process the transaction), and the card brand (*e.g.,* Visa or MasterCard).

of its computer networks and payment card payment processing systems, specifically including the PCI DSS, the Card Brand Rules, and Section 5 of the FTC Act, which are intended to prevent unauthorized disclosure of customers' confidential personal and financial information, and protect issuing financial institution from fraud losses.

**29.** Prior to the Data Breach, highly-publicized data breaches affecting other U.S. retail businesses—such as the Target data breach—put Schnucks on notice of the urgent need to properly secure and monitor its computer network and payment card processing systems. Schnucks knew full well its data security policies, procedures and protocols were inadequate, yet, in the name of cost savings and avoiding any disruption in its business, did nothing to upgrade and improve these policies, procedures and protocols.

**30.** The PCI DSS is the industry data security standard applicable to all entities, including merchants like Schnucks, that store, process, or transmit payment card data. As a merchant that accepts payment cards, Schnucks was at all times contractually obligated by the Card Brand Rules to comply with the PCI DSS.

**31.** The PCI DSS consists of twelve specific security standards that require, in basic terms, (i) installing and maintaining firewalls and network segmentation to protect payment card data, (ii) replacing vendors' default passwords and security parameters, (iii) protecting stored payment card data, (iv) encrypting transmission of payment card data and other sensitive customer data across public networks, (v) using and regularly updating antivirus software on all workstations and servers, (vi) developing and maintaining secure systems and applications, including by installation of the latest vendor-supplied security patches, (vii) restricting access to cardholder data, (viii) assigning unique user credentials to each person with access to any

computer and requiring two-factor authentication[20] for remote access; (ix) restricting physical access to payment card data, (x) tracking and monitoring all access to network resources and payment card data, (xi) regularly testing security systems and processes, and (xii) maintaining policies addressing information security, including for notification to the card brands of an actual or potential payment card data security breach.[21]

**32.** 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.[22]

**33.** As discussed below, Schnucks failed to comply with the PCI DSS and, as a result, hackers accessed and obtained unencrypted payment card data from 2.4 million cards swiped at 79 of Schnucks' stores in in Missouri, Illinois, Indiana, Iowa, and Wisconsin between December 1, 2012 and March 30, 2013. Fraudsters used the compromised payment card information to make fraudulent transactions around the world, inflicting substantial damages and other actual injury and harm on Plaintiffs and Class Members as alleged herein.

---

[20] Two-factor authentication is a system that requires users to provide two different types of credentials in order to gain access. A common example is an ATM machine, which requires not only a memorized PIN code, but also a physical debit card. In the context of payment card processing environments, this often means requiring a user password plus a physical smart card or USB key, the combination of which is vastly more secure than requiring a password alone, to gain access to card processing systems. *See Data Breaches Can Be Prevented With One Simple Solution,* http://www.pcworld.com /article/2871241/data-breaches-can-be-prevented-with-one-simple-solution.html (last visited October 5, 2016) ("In the case of breaches like Target, or Home Depot, or Sony, the attackers were able to obtain valid username and password credentials to access the network, and the rest is history.").

[21] *See PCI Quick Reference Guide,* https://www.pcisecuritystandards.org/pdfs/pci_ssc_ quick_ guide.pdf (last visited October 5, 2016).

[22] *Schnucks Breach Will Likely Cost Millions*, http://www.stltoday.com/business/local/ schnucks-breach-will-likely-cost-millions/article_a1cbd2d9-7105-5bfe-8d97-07e2d1381bab.html (last visited January 13, 2015).

**34.** The PCI DSS and the Card Brand Rules also require Schnucks to immediately notify Visa and MasterCard (directly or via its acquiring bank) of any actual or potential breach in its payment card data security, and take steps to promptly isolate and remediate any breach.

**35.** The Missouri, Illinois, Indiana, Iowa and Wisconsin data breach notification statutes[23] similarly required Schnucks to notify consumers of a payment card data security breach without unreasonable delay.

**36.** The aforementioned payment card data security and data breach notification requirements are intended to protect both consumers and issuing financial institutions from identity theft and fraud losses. Schnucks is well aware that Plaintiffs and Class Members relied on its compliance with these requirements to avoid fraud losses, and knows that its failure to comply with these requirements would (and did) cause Plaintiffs and Class Members to suffer substantial damages and other actual injury and harm.

**37.** When Visa and MasterCard learn of a potential data security breach, they notify issuing financial institutions so the financial institutions can take steps to prevent fraud losses, including declining transactions, canceling and reissuing compromised payment cards, and warning their customers if need be. MasterCard notifies affected issuers through a Security Alert while Visa notifies affected issuers via a "Compromised Account Management Systems Alert," or "CAMS Alert." These alerts include information about the type of compromised data, the relevant timeframe, and a list of payment card numbers that may have been exposed.

**38.** Issuing financial institutions take the same steps to prevent fraud losses when they learn about a payment card data security breach that could potentially affect their customers' accounts, *e.g.*, via merchant press releases or media reports disclosing a breach.

---

[23] MO. REV. STAT. § 407.1500.1; 815 ILL. COMP. STAT. § 530/10; IND. CODE § 24-4.9-3-3; IOWA CODE § 715C.2; WIS. STAT. § 134.98.

**39.** As discussed below, Schnucks did not comply with the aforementioned notification requirements and did not, in fact, notify any of its customers or the public of the Data Breach until ***more than two weeks*** after it actually learned that payment cards used at its stores—which were issued by Plaintiffs and Class Members—had been compromised and were being used to make fraudulent purchases. Nevertheless, and quite incredibly, during this period, Schnucks continued to accept and process tens of thousands of payment card transactions ***per day*** at its 79 affected stores—even though Schnucks knew that track data from each of such payment cards would almost surely be compromised due to the ongoing Data Breach. This, in fact, happened. Schnucks' wrongful conduct and deceit prevented Plaintiffs and Class Members from taking steps to prevent additional fraud losses, thereby causing them to suffer substantial additional damages and other actual injury and harm.

## III. The Data Breach could not (and would not) have occurred if Schnucks had complied with the PCI DSS, the Card Brand Rules, and Section 5 of the FTC Act.

**40.** Unlike other merchants that have experienced a data breach, Schnucks publicly disclosed few details about the Data Breach, claiming it "did not want to provide a road map for other hackers."[24] Schnucks—and only Schnucks—controls the flow of information and the details about the Data Breach. The only way Plaintiffs may obtain more specific facts about the circumstances surrounding the Data Breach is through discovery.

**41.** What is clear, however, is that sometime prior to December 9, 2012, fraudsters gained access to Schnucks' computer network in Missouri and installed malicious software ("malware") on an employee workstation connected to the internet. Malware, for example, infects a computer when a user at a workstation clicks on a hyperlink in an email or otherwise

[24] *Schnucks Breach Will Likely Cost Millions,* http://www.stltoday.com/business/local/schnucks-breach-will-likely-cost-millions/article_a1cbd2d9-7105-5bfe-8d97-07e2d1381bab.html (last visited January 13, 2015).

visits a web page infected with virus code.[25]

**42.** Once installed, the hackers used the malware to exploit multiple basic infirmities in Schnucks' network security, access sensitive payment card processing systems, and collect and harvest track data, including account numbers, expiration dates, and CVV security codes, of as many as 2.4 million payment cards swiped at 79 different Schnucks locations in Missouri, Illinois, Indiana, Iowa, and Wisconsin between December 9, 2012 and March 30, 2013.[26] None of this could (or would) have happened if Schnucks had complied with the PCI DSS, the Card Brand Rules, and Section 5 of the FTC Act.

**43.** Had Schnucks deployed the required antivirus software (which would have detected and prevented malware installation and propagation), the malware could not (and would not) have infected its computers, and collected and harvested the payment card track data.

**44.** Had Schnucks complied with the PCI DSS network segmentation and firewall requirements, hackers could not possibly have accessed highly-sensitive payment card processing systems in 79 remote locations even if malware had infected internet-connected computers. Indeed, the whole purpose of network segmentation – splitting a computer network into isolated subnetworks that are inaccessible to each other – is to prevent precisely what happened here. The fact that malware was able to access sensitive payment card processing systems in more than 79 remote locations confirms that Schnucks was not PCI DSS compliant.

**45.** Had Schnucks implemented two-factor authentication for remote access to its payment card processing systems, the hackers could not (and would not) have gained remote

---

[25] *See id.; Schnucks Breach Happened When Cards Were Awaiting Approval,* http://www.stltoday.com/business/local/schnucks-breach-happened-when-cards-were-awaiting-approval/article_98fb4519-1d3f-5a10-9735-e698090ddc07.html (last visited October 5, 2016).

[26] *See id.;* Schnucks Press Release (August 11, 2014), https://www.schnucks.com/Press-Releases/?pageNumber=0&seg=&Category=Press.Release&NewsID=334 (last visited October 5, 2016).

access to these systems and obtained customers' track data without possessing two different types of credentials (*e.g.*, a password and a physical smart card or USB key). The fact that hackers were able to do so also confirms that Schnucks was not PCI DSS compliant.

**46.** Moreover, the fact that track data was used in fraudulent transactions across the globe confirms that it was unencrypted and improperly stored. Because the compromised payment card information was not encrypted, the fraudsters had unencumbered access to, and use, of it. Had Schnucks encrypted and properly stored the data, the hackers could not have used it to perpetrate fraud even after they managed to obtain it.

**47.** And had Schnucks tracked and monitored all access to its network resources and payment card data, the hackers could not (and would not) have accessed and harvested the data without detection. If Schnucks had complied with any of these requirements, the Data Breach could not (and would not) have occurred—and Plaintiffs and Class Members would not have suffered the damages they have suffered. Nor did Plaintiffs and Class Members have access to Schnucks' payment card processing systems to insure Schnucks' compliance with the PCI DSS, Card Brand Rules, and Section 5 of the FTC Act.

**48.** As described above, at the time of the Data Breach, Schnucks knowingly or recklessly failed to comply with the PCI DSS, Card Brand Rules, and Section 5 of the FTC Act.

**49.** The Data Breach also could have (and would have) been prevented had Schnucks instituted an effective Enterprise Risk Management ("ERM") system supported by the appropriate ERM software. With an effective ERM process, the risk of a data breach would have been documented and assessed in a way that would have provided transparency to Schnucks' senior management who, in turn, would have had the time and opportunity to take steps to prevent the Data Breach before it occurred. Schnucks, however, knowingly or recklessly failed and refused to develop and implement an effective ERM system.

## IV. Schnucks' deliberate concealment of the ongoing Data Breach caused the Financial Institutions and Class Members to suffer significant additional damages.

**50.** According to its press releases and news accounts,[27] Schnucks first learned of the ongoing Data Breach on March 14, 2013, when its payment card processor alerted it to fraudulent charges on payment cards that had been used at Schnucks grocery stores.

**51.** On March 19, 2013, after it had received additional reports of fraudulent charges on payment cards used at its stores, Schnucks retained Mandiant, a forensic investigation firm.

**52.** Schnucks continued to receive reports of fraudulent charges on payment cards used at its stores. On March 20, 2013, Mandiant finally identified the malware on Schnucks' internal computer and payment card processing systems that allowed the hackers to access and obtain the compromised payment card information. Schnucks, however, did not notify its customers, Plaintiffs, or Class Members of any of this.

**53.** Instead, Schnucks deliberately withheld information regarding the ongoing Data Breach for another ten days—until March 30, 2013—when it finally issued a press release publicly acknowledging the Breach. According to Schnucks, the Data Breach was, by then, finally contained. But that's according to Schnucks, and Schnucks has been less than candid with consumers, Plaintiffs, and Class Members about the Data Breach.

**54.** Schnucks knew full well that its failure to disclose the ongoing Data Breach until March 30, 2013 would cause Plaintiffs and Class Members to incur significant additional damages that they could have (and would have) avoided (by declining authorization and/or cancelling payment cards) had Schnucks promptly disclosed that payment cards used at its stores had been (and continued to be) compromised by the ongoing Data Breach.

---

[27] *See, e.g., Schnucks Supermarket Chain Struggled to Find Breach That Exposed 2.4M Cards,* http://www.computerworld.com/article/2496705/cybercrime-hacking/schnucks-supermarket-chain-struggled-to-find-breach-that-exposed-2-4m-cards.html (last visited October 5, 2016).

**55.** In press releases issued after March 30, 2013, Schnucks reported that 2.4 million payment cards used at affected stores from December 2012 to March 29, 2013 were compromised by the Data Breach.

**56.** Taking Schnucks at its word, the Data Breach lasted for 119 days. That means that on average, more than 20,000 payment cards were compromised at Schnucks' retail grocery stores each day of the Data Breach. At this rate, Schnucks' egregious behavior is even more magnified by the fact that during the more than two weeks between March 14, 2013, the date Schnucks claims it first learned about the Data Breach, and March 30, 2013, when Schnucks first publicly disclosed the Data Breach, over 340,000 payment cards issued by Plaintiffs and Class Members were needlessly compromised without any warning by Schnucks.

**57.** In fact, Schnucks knew its affirmative failure and refusal to disclose the Data Breach – even after it knew it was happening and ongoing – would cause Plaintiffs and Class Members to incur substantial additional damages every single day. In press releases and numerous radio and television spots aired on or after March 30, 2013, Schnucks stated, among other things:

- "Cards used before March 30 are still subject to fraud unless cancelled and a new number reissued"; and
- "The best way to avoid fraudulent charges as a result of this incident is to obtain a new card number."

**58.** Once Schnucks learned about the Data Breach on March 14, 2013, not only did it affirmatively fail to timely notify its customers, Plaintiffs, and Class Members about the ongoing Breach so they could take appropriate steps to avoid additional fraud-related damages, Schnucks also affirmatively failed and refused to take even the most basic step possible to protect its customers, Plaintiffs, and Class Members from additional financial harm—such as posting the following old fashioned, low-tech sign on the front doors and at the cash registers of its stores:

*Sorry…*

**CASH OR CHECKS ONLY!**

NO BANK CARDS ACCEPTED AT THIS TIME!

*We sincerely apologize for any inconvenience.*

**59.** Schnucks did not post this sign and stop accepting payment cards at affected stores after learning about the Data Breach because it knew that doing the right thing would be bad for business. Schnucks derives the majority of its revenue from electronic payment card transactions. By not disclosing the Data Breach, not posting the above sign in its stores, not otherwise warning its customers, and not declining to accept payment cards until the Data Breach could be contained and stopped, Schnucks shifted the financial burden of its wrongful conduct to its customers, Plaintiffs, and Class Members.

**60.** During this period alone (*i.e.*, post-March 13, 2013), Plaintiffs and Class Members incurred substantial Data Breach-related damages in the form of, *inter alia*, fraudulent charges posted to their customers' accounts and "chargeback" fees.

**61.** Although Schnucks' affirmative failure and refusal to comply with the PCI DSS, Card Brand Rules, and Section 5 of the FTC Act provided it with benefits in the form of the cost savings of compliance, such savings were to the financial detriment of the Plaintiffs and Class Members—which have suffered (and will continue to suffer) damages to their businesses and

property in the form of, *inter alia*, (i) the time and out-of-pocket expenses to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest and transaction fees due to reduced payment card usage.

## CLASS ACTION ALLEGATIONS

**62.** Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action against Schnucks as a national class action, for themselves and all members of the following Class of similarly situated payment card issuers (the "Nationwide Class"):

> All banks, savings banks, credit unions, financial institutions and other entities that (i) issued Visa or MasterCard branded credit cards or debit cards that were wrongfully disclosed and compromised in the Schnucks Data Breach, (ii) cancelled and re-issued the compromised payment cards, and/or (iii) reimbursed unauthorized charges made on the compromised payment cards and/or paid "chargeback" fees related to such unauthorized charges.

**63.** Pursuant to Rule 23 of the Federal Rules of Civil Procedure and the laws of the respective states listed below, Plaintiffs also bring this action against Schnucks on behalf of themselves and all members of the following sub-classes of similarly situated payment card issuers (together, the "State Sub-Classes"):

> **ILLINOIS.** All banks, savings banks, credit unions, financial institutions and other entities in Illinois that (i) issued Visa or MasterCard branded credit cards or debit cards that were wrongfully disclosed and compromised in the Schnucks Data Breach, (ii) cancelled and re-issued the compromised payment cards, and/or (iii) reimbursed unauthorized charges made on the compromised payment cards and/or paid "chargeback" fees related to such unauthorized charges (the "Illinois Sub-Class").
>
> **MISSOURI.** All banks, savings banks, credit unions, financial institutions and other entities in Missouri that (i) issued Visa or MasterCard branded credit cards or debit cards that were wrongfully disclosed and compromised in the Schnucks Data Breach, (ii) cancelled and re-issued the compromised payment cards, and/or (iii) reimbursed unauthorized charges made on the compromised payment cards

and/or paid "chargeback" fees related to such unauthorized charges (the "Missouri Sub-Class").

**64.** Excluded from the Nationwide Class and State Sub-Classes are Schnucks and any entity in which Schnucks has an ownership interest.

**65.** The proposed Nationwide Class and State Sub-Classes consist of hundreds of geographically dispersed members, the joinder of which in one action is impracticable. The precise number and identities of the Class Members are currently unknown to Plaintiffs, but can easily be derived from the list of compromised payment cards and their issuers Schnucks has already compiled, and Schnucks, Visa, or MasterCard notified about the Breach.

**66.** Schnucks violated the rights of each Class Member in the same way by its above-described uniform wrongful actions, inaction, and omissions.

**67.** There are questions of law and fact common to the proposed Nationwide Class and State Sub-Classes as a whole that predominate over any questions affecting individual Class Members including, *inter alia*:

(i) whether Schnucks' above-described wrongful actions, inaction, and omissions constitute negligence/gross negligence at common law;

(ii) whether Schnucks' above-described wrongful actions, inaction, and omissions constitute negligence *per se* at common law;

(iii) whether Schnucks' above-described wrongful actions, inaction, and omissions constitute breach of implied contract at common law;

(iv) whether Schnucks' above-described wrongful actions, inaction, and omissions constitute breach of contract(s) to which Plaintiffs and Class Members are third-party beneficiaries;

(v) whether Schnucks' above-described wrongful actions, inaction, and omissions violated the Illinois Consumer Fraud and Deceptive Business Practices Act;

(vi) whether Schnucks should be compelled to refund (or disgorge) the amounts by which it has been unjustly enriched or compelled to make restitution under the common law equitable doctrine of assumpsit and/or under principles of equity;

(vii) whether Schnucks' above-described wrongful actions, inaction, and omissions

directly or proximately caused Plaintiff and Class Members to suffer damages and other actual injury and harm;

(viii) whether Plaintiffs and Class Members are entitled to recover actual damages, consequential damages, incidental damages, statutory damages, punitive damages, pre- and post-judgment interest, attorneys' fees, litigation expenses, and court costs and, if so, the amount of the recovery; and

(ix) whether Plaintiffs and Class Members are entitled to declaratory and injunctive relief.

**68.** Plaintiffs' claims are typical of Class Members' claims because Plaintiffs and Class Members are all victims of Schnucks' above-described wrongful conduct.

**69.** Plaintiffs and their counsel will fairly and adequately represent the interests of Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, those of any of the Class Members. Plaintiffs' counsel are experienced in leading and prosecuting class actions and complex commercial litigation, including data breach cases involving financial institutions.

**70.** A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been (and will continue to be) harmed as a direct and proximate result of Schnucks' above-described wrongful actions, inaction, and omissions. Litigating this case as a class action is appropriate because (i) it will avoid a multiplicity of suits and the corresponding burden on the courts and Parties, (ii) it would be virtually impossible for all Class Members to intervene as parties-plaintiff in this action, (iii) it will allow numerous entities with claims too small to adjudicate on an individual basis because of prohibitive litigation costs to obtain redress for their injuries, and (iv) it will provide court oversight of the claims process once Schnucks' liability is adjudicated.

**71.** Class Members are readily ascertainable since they have all been notified that payment cards issued by them were compromised by the Schnucks Data Breach, whereupon they, *inter alia*, cancelled and re-issued such compromised payment cards, reimbursed fraudulent charges made on the compromised payment cards and/or paid "chargeback" fees related to such

fraudulent charges.

**72.** Certification, therefore, is appropriate under FED. R. CIV. P. 23(b)(3) because the above-described common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

**73.** Certification also is appropriate under FED. R. CIV. P. 23(b)(2) because Schnucks has acted (or refused to act) on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

**74.** Certification also is appropriate under FED. R. CIV. P. 23(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Schnucks. For example, one court might decide that the challenged actions are illegal and enjoin Schnucks, while another court might decide that the same actions are not illegal. Individual actions also could be dispositive of the interests of the other Class Members that were not parties to such actions, and substantially impair or impede their ability to protect their interests.

**75.** Schnucks' above-described wrongful actions, inaction, and omissions are applicable to the Class as a whole, for which Plaintiffs seek, *inter alia*, damages and equitable remedies.

**76.** Absent a class action, Schnucks will retain the benefits of its wrongdoing despite seriously violating the law, and inflicting substantial damages and other actual injury and harm on Plaintiffs and Class Members.

## CLAIMS FOR RELIEF/ CAUSES OF ACTION

### COUNT I

### NEGLIGENCE/GROSS NEGLIGENCE
### (On Behalf of the Nationwide Class under Missouri Law and, Alternatively, the Missouri Sub-Class under Missouri Law)

**77.** The preceding factual statements and allegations are incorporated by reference.

**78.** To establish a negligence claim under Missouri law, there must be (i) a legal duty on the part of the defendant to conform to a certain standard of conduct to protect others against unreasonable risks, (ii) a breach of that duty, (iii) a proximate cause between the conduct and the resulting injury, and (iv) actual damages to the claimant's person or property. *Hoover's Dairy, Inc. v. Mid–Am. Dairymen, Inc.*, 700 S.W.2d 426, 431 (Mo. 1985). Foreseeability that an injury might result from the act complained of normally serves as the paramount factor in determining the existence of a duty. *Id*. (citations omitted). When deciding if some injury was reasonably foreseeable, whether expressly or implicitly, courts examine what the actor knew or should have known. *Id*. (citations omitted).

**79.** By receiving and possessing its customers' private, non-public, confidential, and sensitive payment card information and other customer data, Schnucks knew (or at the very least) should have known, that if it failed to exercise reasonable care and properly safeguard and protect such payment card information and other customer data and a data breach resulted—such as the Data Breach here—the underlying payment cards would be compromised, and Plaintiffs and Class Members would suffer the damages and other actual injury and harm they, in fact, have suffered.

**80.** It was imminently foreseeable to Schnucks that if a data breach occurred, in which payment cards were compromised, that the issuing financial institutions—Plaintiffs and Class Members—would be harmed. There is no other foreseeable group of parties that could be

injured by a data breach when compromised payment cards must be canceled and re-issued, fraudulent charges reimbursed, and "chargeback" fees paid. As such, Schnucks had a legal duty to Plaintiffs and Class Members to comply with certain standards of conduct—*e.g.*, the PCI DSS, the Card Brand Rules, and Section 5 of the FTC Act—and protect them from the damages and other actual injury and harm described above that would (and did) result from a data breach.

**81.** The duty to comply with these standards of conduct and protect Plaintiffs and Class Members from the damages and other actual injury and harm that would result from a data breach also arose out of the business relationship between the parties resting on sound public policy as derived from a calculus of factors, including, *inter alia*, the social consensus that payment cards are worthy of protection (they are), the foreseeability of harm and the degree of certainty that the protected parties suffered injury (the damages and other actual injury and harm suffered by Plaintiffs and Class Members—as the issuers of the compromised payment cards—was imminently foreseeable by Schnucks as the result of the Data Breach), moral blame society attaches to the conduct (data breaches are looked upon with disfavor), and the prevention of future harm (future injury and harm could very well occur if Schnucks does not comply with the PCI DSS, the Card Brand Rules, and Section 5 of the FTC Act—especially since it has yet to adopt EMV chip card technology). *See, e.g.*, *Hoover's Dairy, Inc.*, 700 S.W.2d at 432.

**82.** Taking Schnucks at its word, the Data Breach lasted for 119 days. Schnucks claims it first learned about the Data Breach on March 14, 2013. Thus, and at the very least, as of March 14, 2013, Schnucks knew (or should have known) that Plaintiffs' and Class Members' damages and other actual injury and harm resulting from the Data Breach were imminent—yet it did not publicly disclose the Data Breach until more than two weeks later on March 30, 2013. During that time, on the average, over 340,000 payment cards issued by Plaintiffs and Class Members were needlessly compromised without any warning by Schnucks. Thus, at the very

least, as of March 14, 2013, Schnucks knew it had a legal duty to protect Plaintiffs and Class Members from the damages and other actual injury and harm that would result from the Breach.

**83.** As discussed in detail above, Schnucks also had a duty to timely disclose to Plaintiffs and Class Members that the Data Breach had occurred, and their private, non-public, confidential and sensitive payment card information and other customer data had been wrongfully disclosed and compromised—so that Plaintiffs and Class Members could take the appropriate steps necessary to minimize their damages by, for example, immediately canceling and re-issuing the compromised payment cards, declining fraudulent charges, and warning their customers—via text, email, or mail—about using payment cards when shopping at Schnucks.

**84.** After learning about the Data Breach, Schnucks also affirmatively failed and refused to take even the most basic steps possible to protect its customers from additional financial harm—such as posting an old fashioned, low-tech warning sign on the front doors and at the cash registers of its stores. *See, e.g.,* ¶ 58, *supra*. Instead, by its above-described wrongful actions, inaction, and omissions, and delayed disclosure of the Data Breach, Schnucks shifted its notification obligation and expenses to Plaintiffs and Class Members. Schnucks also (i) directly and proximately caused Plaintiffs and Class Members to suffer the above-described damages and other actual injury and harm, (ii) saved the cost of implementing the proper payment card security policies, procedures, protocols, and hardware and software systems, and (iii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members.

**85.** Schnucks' above-described duties to Plaintiffs and Class Members also arose from the duties expressly imposed upon Schnucks by other sources, such as industry standards (PCI DSS), best practices, implied contracts between Schnucks and Plaintiffs and Class Members, contracts between Schnucks and third parties (such as Citicorp and First Data), and participation in the Visa and MasterCard Networks (including the Card Brand Rules).

**86.** Schnucks' above-described duties also arose from Section 5 of the FTC Act, which Schnucks violated. Section 5 of the FTC Act prohibits unlawful, unfair, and deceptive acts or practices in or affecting commerce, including, as interpreted and enforced by the FTC, the practice of failing to use reasonable measures to safeguard and protect Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data. Plaintiffs and Class Members "are within the class of persons intended to be protected by the statute, and [] the harm suffered is the kind the statute meant to protect." *See In re The Home Depot, Inc. Customer Data Breach Litig.*, 2016 WL 2897520, at *4 (financial institution case).

**87.** Schnucks negligently, or in a grossly negligent manner, breached its common law, statutory, and other duties to Plaintiffs and Class Members by (i) failing to implement the appropriate payment card data security policies, procedures, protocols, and hardware and software systems across its computer network, (ii) failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' private, non-public, confidential and sensitive payment card information and other customer data in Schnucks' possession, custody and control, and (iii) failing to provide timely notice of the Data Breach. Schnucks' specific negligent and wrongful actions, inaction, and omissions include, *inter alia*:

a. failing to delete payment card information after the time period necessary to authorize a payment card transaction;

b. failing to employ systems to protect against malware;

c. failing to regularly update its antivirus software;

d. failing to maintain an adequate firewall;

e. failing to track and monitor access to its network and cardholder data;

f. failing to limit access to those with a valid purpose;

g. failing to encrypt personally identifiable information, such as the now-

compromised payment card information, at the point-of sale;

h. failing to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

i. failing to assign unique identification numbers to each individual with access to its systems;

j. failing to automate the assessment of technical controls and security configuration standards;

k. failing to adequately staff and fund its data security operation;

l. failing to use due care in hiring, promoting, and supervising those responsible for its data security operations;

m. failing to recognize red flags signaling its systems were inadequate and the resulting potential for a massive data breach akin to the Target and Home Depot data breaches was increasingly likely; and

o. failing to recognize for approximately four months that hackers were obtaining personally identifiable information, such as the now-compromised payment card information, from its computer network while the Data Breach was taking place.

In doing so, Schnucks acted wantonly, recklessly, and with a complete disregard for Plaintiffs' and Class Members' rights and interests and the consequences of its wrongful conduct. The Data Breach was the reasonably foreseeable consequence of Schnucks' above-described wrongful actions, inaction, negligence, and gross negligence.

**88.** As a direct and proximate result of Schnucks' above-described wrongful actions, inaction, omissions, negligence, and gross negligence, Plaintiffs and Class Members have suffered (and will continue to suffer) the above-described damages to their businesses and property, and other injury and actual harm, in the form of, *inter alia*, (i) the time and expense to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest

and transaction fees due to reduced payment card usage

**89.** The economic loss doctrine does not bar Plaintiffs' and Class Members' negligence and gross negligence claims because, *inter alia*, (i) Schnucks is in the business of supplying information to Plaintiffs and Class Members for their guidance in connection with electronic payment card transactions made at Schnucks' stores utilizing payment cards issued by Plaintiffs and Class Members, about and for which Schnucks regularly communicates with Plaintiffs and Class Members via the interstate wires to secure authorization of such electronic transactions, and (ii) Schnucks breached its above-described duties to safeguard and protect Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data, provide timely notice of the Data Breach, and observe and comply with the PCI DSS, The Card Brand Rules, and Section 5 of the FTC Act.

**90.** Schnucks' above-described wrongful actions, inaction, omissions, and the resulting Data Breach, constitute negligence and gross negligence at Missouri common law.

**COUNT II**

**NEGLIGENCE *PER SE***
**(On Behalf of the Nationwide Class under Missouri Law and, Alternatively, the Missouri Sub-Class under Missouri Law)**

**91.** The preceding factual statements and allegations are incorporated by reference.

**92.** Section 5 of the FTC Act prohibits "unfair … practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, such as Schnucks, of failing to use reasonable measures to safeguard and protect personally identifiable information, such as Plaintiffs' and Class Members' confidential and sensitive payment card information and other customer data. FTC publications and orders also

form the basis of Schnucks' duty.[28]

**93.** By its above-described wrongful actions, inaction, and omissions, to wit, failing to use reasonable measures to protect Plaintiffs' and Class Members' confidential and sensitive payment card information and other customer data, and not complying with applicable industry standards, including PCI DSS, as set forth above, Schnucks violated Section 5 of the FTC Act. Schnucks' wrongful conduct was particularly unreasonable given the nature and amount of unencrypted personally identifiable information, such as the now-compromised payment card information, it obtained and stored, the foreseeable consequences of a data breach at a large, regional retailer (*see, e.g.*, the Target and Home Depot data breaches), and the resulting immense damages suffered by consumers and financial institutions, such as Plaintiffs and Class Members.

**94.** Plaintiffs and Class Members are within the class of persons Section 5 of the FTC Act is designed to protect as they are engaged in trade and commerce, and bear primary responsibility for canceling and re-issuing compromised payment cards and reimbursing

---

[28] For example, in 2007, the FTC first published guidelines, entitled "Protecting Personal Information: A Guide for Business" establishing reasonable data security practices for businesses. *See, e.g.,* https://www.bulkorder.ftc.gov/system/files/publications/bus69-protecting-personal-information-guide-business_0.pdf (last visited Oct. 16, 2016). The guidelines state that businesses should protect the personal customer information they keep, properly dispose of information that is no longer needed, encrypt information stored on computer networks, understand their networks' vulnerabilities, and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating that hackers may be trying to hack the system, watch for large amounts of data being transmitted from the system, and have a data breach response plan in place.

The FTC also has published a document, entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks. The FTC also has issued orders against businesses that failed to employ reasonable measures to secure customer data, all of which provide further guidance to businesses regarding their data security obligations under the FTC. *See also FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 236 (3d Cir. 2015) (affirming that the FTC has authority to regulate cybersecurity in businesses).

consumers for fraud losses. In fact, two of the Plaintiffs and many of the absent Class Members are credit unions organized as cooperatives whose members are consumers.

**95.** Moreover, the damages, injury and harm suffered by Plaintiffs and Class Members are the types of damages, injury and harm the FTC Act is intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same injury and harm suffered by Plaintiffs and Class Members here.

**96.** By its above-described wrongful actions, inaction, and omissions, Schnucks also failed to comply with industry best practices, the PCI DSS, and the Card Brand Rules. Plaintiffs and Class Members are members of the classes of persons intended to be protected by the PCI DSS, the Card Brand Rules, and other industry data security standards and best practices. The damages and other actual injury and harm suffered by Plaintiffs and Class Members are the types of damages, injury, and harm that industry best practices, the PCI DSS, and the Card Brand Rules are intended to guard against.

**97.** Schnucks' violations of Section 5 of the FTC Act, industry best practices, the PCI DSS, and the Card Brand Rules constitute negligence *per se* at Missouri common law.[29]

**98.** As a direct and proximate result of Schnucks' above-described negligence *per se*, Plaintiffs and Class Members have suffered (and will continue to suffer) damages to their businesses and property, and other actual injury and harm, in the form of, *inter alia*, (i) the time and expense to (a) cancel and reissue compromised payment cards, (b) change or close accounts,

---

[29] *See In re The Home Depot, Inc. Customer Data Breach Litig.*, 2016 WL 2897520, at *4 ("The Consolidated Class Action Complaint here adequately pleads a violation of Section 5 of the FTC Act, that the Plaintiffs are within the class of persons intended to be protected by the statute, and that the harm suffered is the kind the statute meant to protect."). Plaintiffs' and Class Members' negligence *per se* allegations are virtually identical to the financial institution plaintiffs' negligence *per se* allegations in *Home Depot*. *See id*., Doc. #104, Count II, ¶¶ 216-22.

(c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest and transaction fees due to reduced payment card usage.

**COUNT III**

**BREACH OF IMPLIED CONTRACT**
**(On behalf of the Nationwide Class under Missouri Law and, Alternatively, the Missouri Sub-Class under Missouri Law and the Illinois Sub-Class under Illinois Law)**

**99.** The preceding factual statements and allegations are incorporated by reference.

**100.** Schnucks required payment card data and other confidential customer data compromised by the Data Breach to facilitate electronic payment card transactions, and thereby derive substantial revenue and profits.

**101.** Schnucks requested Plaintiffs' and Class Members' authorization of tens of thousands of payment card transactions over the Visa and MasterCard Networks each day in exchange for the payment of interchange fees and other valuable consideration described herein.

**102.** Plaintiffs' and Class Members' authorization of these transactions was contingent upon Schnucks' implicit promises to take reasonable efforts to safeguard and protect the confidential and sensitive payment card information and other customer data, and promptly notify Plaintiffs and Class Members in the event the payment card information and other customer data was disclosed and compromised in a data breach.

**103.** Plaintiffs and Class Members lived up to their obligations by reviewing and authorizing millions of electronic payment card transactions via the Visa and MasterCard Networks. Notwithstanding its above-described obligations, however, Schnucks knowingly or recklessly (i) failed to safeguard and protect Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data, (ii) failed to

comply with the PCI DSS, the Card Brand Rules, and Section 5 of the FTC Act, (iii) failed to immediately notify Visa, MasterCard, financial institutions, or the public about the ongoing Data Breach after discovering it and despite knowing that tens of thousands of payment cards issued by Plaintiffs and Class Members were being compromised each day, and (iv) failed to take steps to promptly isolate and remediate the Breach during the approximately two week period when Schnucks knew it was ongoing.

**104.** Had Plaintiffs and Class Members known that Schnucks had not properly safeguarded and protected its payment card systems and the now-compromised payment card information, or that it was continuing to accept payment cards in affected stores despite full knowledge its payment card systems, in fact, had been compromised, Plaintiffs and Class Members would have declined payment card transactions, cancelled and re-issued compromised payment cards, and/or notified their customers to stop using payment cards at Schnucks—thereby avoiding the damages and other actual injury and harm they have suffered.

**105.** Schnucks' above-described wrongful actions, inaction, and omissions directly and proximately caused Plaintiffs and Class Members to suffer damages to their businesses and property, and other actual injury and harm, in the form of, *inter alia*, (i) the time and expense to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest and transaction fees due to reduced payment card usage.

**106.** Schnucks' above-described wrongful actions, inaction, and omissions, and the resulting Data Breach, constitute breach of implied contract at common law.

**COUNT IV**

**BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS ARE THIRD-PARTY BENEFICIARIES**
**(On behalf of the Nationwide Class under Missouri Law and, Alternatively, the Missouri Sub-Class under Missouri Law and the Illinois Sub-Class under Illinois Law)**

**107.** The preceding factual statements and allegations are incorporated by reference.

**108.** At all relevant times, Schnucks was (and continues to be) bound by the Card Brand Rules and other agreements between it, its acquiring bank, and the Visa and MasterCard Networks to comply with the PCI DSS and Card Brand Rules, immediately notify the card brands (directly or via its acquiring bank) of any actual or potential breach in payment card data security, and take specific steps to promptly isolate and remediate any breach.

**109.** Plaintiffs and Class Members are intended third-party beneficiaries of these agreements because, pursuant to the agreements, they earn interchange fees and/or interest when their customers use payment cards at Schnucks stores, and Schnucks' failure to comply with the PCI DSS and Card Brand Rules could (and would) result in foreseeable and substantial harm to Plaintiffs and Class Members—which, in fact, happened (as alleged herein).

**110.** Under the circumstances, Plaintiffs' and Class Members' recognition of a right to performance is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiffs and Class Members the benefit of the performance promised in the contracts.

**111.** As described above, Schnucks breached these contracts by, *inter alia*, (i) failing to comply with the PCI DSS, (ii) failing to comply with the Card Brand Rules and Section 5 of the FTC Act, (iii) failing to immediately notify Visa, MasterCard, financial institutions, or the public about the ongoing Data Breach after discovering it and despite knowing that tens of thousands of payment cards issued by Plaintiffs and Class Members were being compromised each day, and (iv) failing to take steps to promptly isolate and remediate the Breach during the approximately

two week period when Schnucks knew it was ongoing.

**112.** By its above-described wrongful actions, inaction, and omissions, and the resulting Data Breach, Schnucks directly and proximately caused Plaintiffs and Class Members to suffer damages to their businesses and property, and other actual injury and harm, in the form of, *inter alia*, (i) the time and expense to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest and transaction fees due to reduced payment card usage.

**113.** By its above-described wrongful actions, inaction, and omissions, and the resulting Data Breach, Schnucks also received (or avoided spending) a substantial sum of money by knowingly failing to comply with its contractual obligations. Schnucks' above-described wrongful actions, inaction, omissions, and the resulting Data Breach constitute breach of contract(s) to which Plaintiffs and Class Members were third-party beneficiaries.

## COUNT V

## VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT

**(On behalf of the Illinois Sub-Class under Illinois Law)**

**114.** The preceding factual statements and allegations are incorporated by reference.

**115.** The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/1, *et seq.* ("ICFA"), prohibits unfair acts or practices. In determining whether an act or practice is unfair, ICFA expressly requires that consideration be given to interpretations made by the FTC pertaining to Section 5 of the FTC Act. *See* 815 Ill. Comp. Stat. 505/2.

**116.** Schnucks engaged in unfair business practices in violation of ICFA by failing to implement and maintain reasonable payment card data security measures, violating industry

standards, such as the PCI DSS, and committing the other above-described wrongful actions, inaction, and omissions that caused the Data Breach.

**117.** Schnucks' above-described wrongful actions, inaction, omissions, and the resulting Data Breach offend public policy; are immoral, unethical, oppressive, or unscrupulous; and caused Plaintiffs and Class Members to suffer substantial damages and other actual injury and harm.

**118.** Schnucks' above-described wrongful actions, inaction, and omissions specifically inflicted substantial damages and other actual injury and harm on Plaintiffs CBT, UIECU, FFSB, the Illinois Sub-Class Members, and Class Members operating in Illinois. Schnucks' above-described wrongful actions, inaction, and omissions also harmed competition. While Schnucks cut corners and minimized costs, its competitors spent the time and money necessary to ensure that confidential and sensitive payment card information and other customer data was properly safeguarded and protected.

**119.** Plaintiffs CBT, UIECU, FFSB, the Illinois Sub-Class Members, and Class Members operating in Illinois reasonably expected Schnucks to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to safeguard and protect the confidential and sensitive payment card information and other customer data wrongfully disclosed and compromised in the Data Breach.

**120.** Schnucks' practice of maintaining inadequate payment card data security measures provided no benefit to Plaintiffs CBT, UIECU, FFSB, the Illinois Sub-Class Members, Class Members operating in Illinois, consumers, and competition in general. The substantial damages and other actual injury and harm sustained by Plaintiffs CBT, UIECU, FFSB, the Illinois Sub-Class Members, and Class Members operating in Illinois are not outweighed by any countervailing benefits to consumers or competition. Further, because Schnucks is directly and

solely responsible for safeguarding and protecting confidential and sensitive payment card information and other customer data, Plaintiffs CBT, UIECU, FFSB, the Illinois Sub-Class Members, and Class Members operating in Illinois could not have known about Schnucks' inadequate payment card data security practices, and thus, could not have avoided the damages and other actual injury and harm suffered by them.

**121.** Schnucks' above-described wrongful actions, inaction, omissions, and unfair acts and practices violated Illinois Consumer Fraud and Deceptive Business Practices Act.[30]

**122.** As a direct and proximate result of Schnucks' above-described wrongful actions, inaction, omissions, and unfair acts and practices, Plaintiffs CBT, UIECU, FFSB, the Illinois Sub-Class Members, and Class Members operating in Illinois have suffered (and will continue to suffer) damages to their businesses and property, and other actual injury and harm, in the form of, *inter alia*, (i) the time and expense to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest and transaction fees due to reduced payment card usage. Plaintiffs CBT, UIECU, FFSB, Illinois Sub-Class Members, and Class Members operating in Illinois also are entitled to attorneys' fees, litigation expenses, costs, and injunctive and declaratory relief.

---

[30] *See In re The Home Depot, Inc. Customer Data Breach Litig.*, 2016 WL 2897520, at *6 ("Addressing a data breach at another national retailer [Michael's Stores], the Northern District of Illinois found that where a plaintiff alleged failure to comply with industry standards, that plaintiff could survive a motion to dismiss a claim under ICFA. That is exactly what the Plaintiffs have alleged here.") (citing *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 525-26 (N.D. Ill. 2011)). Plaintiffs' and Class Members' ICFA allegations are virtually identical to the financial institution plaintiffs' ICFA allegations in *Home Depot*. *See id*., Doc. #104, Count VII, ¶¶ 248-54.

## COUNT VI

## UNJUST ENRICHMENT/ASSUMPSIT
**(On behalf of the Nationwide Class under Missouri Law and, Alternatively, the Missouri Sub-Class under Missouri Law and the Illinois Sub-Class under Illinois Law)**

**123.** The preceding factual statements and allegations are incorporated by reference.

**124.** Plaintiffs plead this Count in the alternative to their contract claims because they cannot recover under this Count and under their contract claims.

**125.** Plaintiffs and Class Members conferred a substantial benefit on Schnucks by authorizing of tens of thousands of payment card transactions over the Visa and MasterCard Networks each day. Schnucks derived tens of millions of dollars in revenue from these transactions during the Data Breach alone.

**126.** At the time it requested Plaintiffs' and Class Members' payment card authorizations, Schnucks knew that they relied on Schnucks to properly secure its payment card processing systems and immediately report any payment card data security breach, so that Plaintiffs and Class Members could take appropriate steps to avoid or minimize fraud losses and other damages, injury, and harm.

**127.** To the extent Schnucks was not contractually obligated to do these things, either by contracts to which Plaintiffs and Class Members were third-party beneficiaries or by contracts implied in fact, equity and justice require that a contract be implied at law to prevent Schnucks' unjust enrichment.

**128.** Plaintiffs' and Class Members' authorization of Schnucks' payment card transactions was contingent upon Schnucks' implicit promises to take reasonable efforts to safeguard and protect confidential and sensitive payment card information and other customer data, and promptly notify Plaintiffs and Class Members in the event payment card information and other customer data was disclosed and compromised.

**129.** At the time it requested Plaintiffs' and Class Members' authorizations, however, Schnucks knew (or should have known) that its payment card systems were not properly secured. At the very least, during the period from March 14, 2013 through March 30, 2013, Schnucks knew that tens of thousands of payment cards issued by Plaintiffs and Class Members were being compromised each day, yet Schnucks failed to take appropriate steps to promptly isolate and remediate the Breach, refused to stop accepting payment cards at its affected stores, and failed to notify Visa, MasterCard, Plaintiffs, Class Members, or the public of the ongoing Breach.

**130.** Indeed, had Schnucks taken the basic step – even after actually learning about the ongoing Data Breach – of posting "Cash or Checks Only" signs and/or refusing to accept payment cards at its 79 affected stores, Schnucks would have lost substantial revenue from payment card transactions—but it would have been the right thing to do because it would have prevented substantial losses to Plaintiffs and Class Members and their customers. Plaintiffs and Class Members canceled and re-issued tens of thousands of payment cards that were compromised during this period alone. Plaintiffs and Class Members also reimbursed their customers for fraudulent charges and/or paid per-transaction "chargeback" fees made on payment cards compromised during this period.

**131.** By accepting payment from Plaintiffs and Class Members during the Data Breach, Schnucks was unjustly enriched by, *inter alia*, (i) the revenue and profits from payment card transactions approved by Plaintiffs and Class Members over card brand networks from December 2012 through March 30, 2013, (ii) the use and investment of the revenue and profits, and (iii) the shifted risk and expense of the Data Breach to Plaintiffs and Class Members. During this same period, Plaintiffs and Class Members, on the other hand, suffered tens of millions of dollars in losses as described herein. Schnucks' acceptance and retention of these revenues and profits at the expense of Plaintiffs and Class Members would be unjust and inequitable.

**132.** Schnucks, therefore, as a matter of justice, equity, and good conscience, should be compelled to refund (or disgorge) such wrongfully earned revenues, profits, and earnings under the common law doctrine of unjust enrichment, the duty to make restitution under the common law equitable doctrine of assumpsit, and/or general principles of equity.

## COUNT VII

## DECLARATORY AND INJUNCTIVE RELIEF
**(On behalf of the Nationwide Class and, Alternatively, the State Sub-Classes)**

**133.** The preceding factual statements and allegations are incorporated by reference.

**134.** Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, the Court is authorized to enter a judgment declaring the Parties' rights and legal relations, and grant further necessary relief based upon such a judgment. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the above-alleged state law.

**135.** An actual controversy exists in the wake of the Data Breach regarding Schnucks' duties to safeguard and protect Plaintiffs' and Class Members' confidential and sensitive payment card information and other customer data. Schnucks' payment card data security measures were (and continue to be) woefully inadequate. Indeed, to this day, Schnucks has failed to adopt EMV chip technology.[31] Plaintiffs and Class Members could very well continue to

---

[31] EMV—which stands for Europay, MasterCard and Visa—is the global standard for credit card and debit card payments. Chip cards use imbedded computer chips, rather than magnetic strips, to authenticate electronic payment card transactions. Following an October 1, 2015 deadline established by major U.S. credit card issuers MasterCard, Visa, Discover, and American Express (which Schnucks has missed by over a year), the liability for card-present fraud shifted to whichever party is the least EMV-compliant in a fraudulent transaction. If, for example, a financial institution issued a chip card used at Schnucks, which is not EMV chip technology enabled, the cost of any fraud will fall back on Schnucks. The change is intended to encourage the entire payment industry to adopt chip technology by encouraging compliance to avoid liability costs. Such encouragement has been lost on Schnucks.

suffer damages and other actual injury and harm as additional fraudulent charges are made on payment cards issued by Plaintiffs and Class Members used to make purchases at Schnucks.

**136. DECLARATORY RELIEF.** Pursuant to its authority under the Declaratory Judgment Act, Plaintiffs and Class Members request the Court to enter a judgment declaring, *inter alia*, (i) Schnucks owed (and continues to owe) a legal duty to safeguard and protect Plaintiffs' and Class Members' confidential and sensitive payment card information and other customer data, and timely notify financial institutions about data breaches under the common law, Section 5 of the FTC Act, the PCI DSS, the Card Brand Rules, industry best practices, state statutes, and its commitments, (ii) Schnucks breached (and continues to breach) such legal duties by failing to employ reasonable measure to safeguard and protect Plaintiffs' and Class Members' confidential and sensitive payment card information and other customer data secure, and make the requisite notifications, (iii) Schnucks' breach of its legal duties directly and proximately caused the Data Breach, and (iv) financial institutions that cancelled and re-issued payment cards compromised by the Breach, reimbursed fraudulent charges made on the compromised payment cards, and/or paid "chargeback" fees care legally entitled to recover compensation for their damages and other actual injury and harm from Schnucks.

**137. INJUNCTIVE RELIEF.** The above-described repetitious and systematic wrongful acts engaged in by Schnucks has caused (and will continue to cause) Plaintiffs and Class Members to suffer irreparable harm in the form of, *inter alia*, (i) the time and expense to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest and transaction fees due to reduced payment card usage. Such irreparable harm will not cease

unless and until enjoined by this Court. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and other appropriate affirmative relief including, *inter alia*, an order compelling Schnucks to (i) immediately comply with the PCI DSS, the Card Brand Rules, Section 5 of the FTC Act, and industry best practices, (ii) pay restitution or disgorge its gross revenue from electronic payment card transactions made on the payment cards wrongfully disclosed and compromised by the Data Breach, and all other amounts by which Schnucks have been unjustly enriched, and (iii) discontinue its above-described wrongful actions, inaction, and omissions.

**138.** Plaintiffs and Class Members also are entitled to injunctive relief requiring Schnucks to implement and maintain payment card data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (a) employing strong industry standard encryption algorithms for encryption keys providing access to stored payment card information, (b) using its encryption keys in accordance with industry standards, (c) immediately encrypting the payment card information currently in its possession, custody and control, (d) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Schnucks' computer systems on a periodic basis, (e) engaging third-party security auditors and internal personnel to run automated security monitoring, (f) auditing, testing, and training its security personnel regarding any new or modified procedures, (g) segmenting payment card information by, among other things, creating firewalls and access controls so that if one area of Schnucks is compromised, fraudsters cannot gain access to other portions of Schnucks' computer systems, (h) purging, deleting, and destroying in a reasonably secure manner all payment card information not necessary to consummate sales transactions, (i) conducting regular database scanning and security checks, (j) regularly evaluating web applications for vulnerabilities to prevent web application threats, and (k) periodically conducting internal training and education

to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response. The Court also should issue injunctive relief requiring Schnucks to employ adequate security protocols consistent with industry rules and standards to protect its customers' personal and financial information—including the adoption and implementation of EMV chip technology.

**139.** If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury in the event of another Schnucks data breach, the risk of which is real, immediate, and substantial.

**140.** The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Schnucks if an injunction is issued. Among other things, if another massive data breach occurs at Schnucks, Plaintiffs and Class Members will likely again incur millions of dollars in damages. On the other hand, and setting aside the fact that Schnucks has a pre-existing legal obligation to employ adequate payment card data security measures, the cost to Schnucks of complying with an injunction requiring the institution of such data security measures it is already required to implement is relatively minimal.

**141.** Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another Schnucks data breach, thereby eliminating the damages, injury and harm that would be suffered by Plaintiffs, Class Members, and the millions of consumers whose confidential and sensitive payment card information and other customer data would be compromised.

## RELIEF REQUESTED

**142.** The preceding factual statements and allegations are incorporated by reference.

**143.** **ACTUAL, CONSEQUENTIAL, AND INCIDENTAL DAMAGES AND/OR EQUITABLE RELIEF.** As a direct and proximate result of Schnucks' above-described wrongful actions,

inaction, omissions, and the resulting Data Breach, Plaintiffs and Class Members have sustained (and will continue to sustain) actual, consequential, incidental, and statutory damages to their businesses and property, and other actual injury and harm, in the form of, *inter alia*, (i) the time and expense to (a) cancel and reissue compromised payment cards, (b) change or close accounts, (c) notify customers that their payment cards were compromised, and (d) investigate claims of fraudulent activity, (ii) reimbursement of customers for fraudulent charges made on the compromised payment cards and/or "chargeback" fees related to such fraudulent charges, and (iii) lost interest and transaction fees due to reduced payment card usage—for which Plaintiffs and Class Members are entitled to compensation. Alternatively, Plaintiffs and Class Members are entitled to equitable relief in the form of restitution or disgorgement of Schnucks' revenues, profits, or earnings from electronic payment card transactions made on the wrongfully disclosed and compromised payment cards during the Data Breach, and all other amounts by which Schnucks have been unjustly enriched. All of the damages, injuries, and harm sustained by Plaintiffs and Class Members were reasonably foreseeable by Schnucks. All conditions precedent to Plaintiffs' and Class Members' claims for relief have been performed or occurred.

**144. PUNITIVE DAMAGES.** Schnucks' above-described wrongful actions, inaction, omissions, and the resulting Data Breach were committed willfully, wantonly, and with reckless disregard for Plaintiffs' and Class Members' rights and interests. Accordingly, Plaintiffs and Class Members are entitled to punitive damages from Schnucks as punishment, and to discourage such wrongful conduct in the future. All conditions precedent to Plaintiffs' and Class Members' claims for relief have been performed or occurred.

**145. DECLARATORY AND INJUNCTIVE RELIEF.** Plaintiffs and Class Members also are entitled to declaratory and injunctive relief (as set forth above). All conditions precedent to Plaintiffs' and Class Members' claims for relief have been performed or occurred.

**146. ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiffs and Class Members also are entitled to recover their attorneys' fees, litigation expenses, and court costs under, *inter alia*, the Illinois Consumer Fraud and Deceptive Business Practices Act, and state statutory and common law. All conditions precedent to Plaintiffs' and Class Members' claims for attorneys' fees, litigation expenses, and court costs have been performed or occurred.

**WHERFORE,** Plaintiffs, for themselves and Class Members, respectfully request that (i) Schnucks be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class Representatives and Sub-Class Representatives, and (iv) Plaintiffs' counsel be appointed Class Counsel. Plaintiffs, for themselves and Class Members, also request that upon final trial or hearing, judgment be awarded against Schnucks in their favor for:

(i) actual, consequential, incidental, and statutory damages to be determined by the trier of fact;

(ii) punitive damages;

(iii) an equitable accounting for all benefits, consideration, revenues, profits, and earnings received, directly or indirectly, by Schnucks from electronic payment card transactions made on the wrongfully disclosed and compromised payment cards during the Data Breach, including the imposition of a constructive trust, the voiding of unlawful transfers, the disgorgement of all ill-gotten revenues, profits, and earnings, and all amounts by which Schnucks have been unjustly enriched;

(iv) declaratory and injunctive relief (as set forth above);

(v) pre- and post-judgment interest at the highest legal rates;

(vi) attorneys' fees, litigation expenses, and costs of suit incurred through the trial and any appeals of this case; and

(vii) such other and further relief the Court deems just and proper.

## JURY DEMAND

Plaintiffs, for themselves and all others similarly situated, respectfully demand a trial by jury on all claims so triable.

Date: October 19, 2016.

Respectfully submitted,

By: */s/ John J. Driscoll*
John J. Driscoll
Christopher J. Quinn
**THE DRISCOLL FIRM, P.C.**
211 N. Broadway, 40th Floor
St. Louis, MO 63102
Telephone: (314) 932-3232
Email: john@thedriscollfirm.com
Email: chris@thedriscollfirm.com

Richard L. Coffman
**THE COFFMAN LAW FIRM**
First City Building
505 Orleans St., Fifth Floor
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

Gary R. Lietz
**LIETZ, BANNER, FORD, LLP**
1605 South State Street, Suite 103
Champaign, IL 61820
Telephone: (217) 353-4900
Facsimile: (217) 353-4901
Email: glietz@lbflaw.com

**ATTORNEYS FOR PLAINTIFFS AND THE PUTATIVE CLASS**

**COUNSEL WAITING FOR ADMISSION *PRO HAC VICE*:**

Mitchell A. Toups
**WELLER, GREEN TOUPS & TERRELL, LLP**
2615 Calder Ave., Suite 400
Beaumont, TX 77702
Telephone: (409) 838□0101
Facsimile: (409) 838□6780
Email: matoups@wgttlaw.com

**OF COUNSEL:**

G. Robert Blakey
Professor of Law Emeritus
Notre Dame Law School*
7002 East San Miguel Ave.
Paradise Valley, AZ 85253
Telephone: (574) 514-8220
Email: blakey.1@nd.edu
* Noted for identification only

**CERTIFICATE OF SERVICE**

I certify that a true and correct copy of Plaintiffs' First Amended Class Action Complaint and Jury Demand was served on all counsel of record, via the Court's electronic filing system, on October 19, 2016.

*/s/ John J. Driscoll*
John J. Driscoll