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**
	§	**JURY TRIAL DEMANDED**
PLAINTIFFS,	§	
	§	**EQUITABLE RELIEF IS SOUGHT**
v.	§	
SCHNUCK MARKETS, INC.,	§	
DEFENDANT.	§	

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

NATURE OF THE CASE 1

JURISDICTION AND VENUE 7

PARTIES 8

FACTS 12

I. Payment Card Transactions on the Visa and MasterCard Networks.....12

II. Prior to the Data Breach, Schnucks also knew its internal computer systems were not compliant with the PCI DSS, Visa Operating Regulations, and MasterCard Rules.....13

III. The Schnucks Data Breach 16

IV. The Schnucks Data Breach never should have happened 18

PATTERN OF UNLAWFUL ACTIVITY (WIRE FRAUDAND MAIL FRAUD) 20

CLASS ACTION ALLEGATIONS 24

CLAIMS FOR RELIEF/CAUSES OF ACTION 28

COUNT I Violation of 18 U.S.C. § 1962(c).....28

COUNT II Violation of 18 U.S.C. § 1962(d) by Conspiring to Violate 18 U.S.C. § 1962(a) 32

COUNT III Violation of 18 U.S.C. § 1962(d) by Conspiring to Violate 18 U.S.C. § 1962(c).....34

COUNT IV Breach of Fiduciary Duty.....36

COUNT V Negligent Misrepresentation 39

COUNT VI Negligence/Gross Negligence.....43

COUNT VII Negligence *Per Se* 45

COUNT VIII Breach of Implied Contract 48

COUNT IX Breach of Contracts to which Plaintiffs are Third-Party Beneficiaries 49

COUNT X Violation of the IL Consumer Fraud and Deceptive Business Practices Act...51

COUNT XI Unjust Enrichment/Assumpsit 53

COUNT XII Equitable Subrogation 54

COUNT XIII Declaratory and Injunctive Relief 55

RELIEF REQUESTED.....58

Plaintiffs Community Bank of Trenton, University of Illinois Employees Credit Union, First Federal Savings Bank of Champaign-Urbana, and Southpointe Credit Union (collectively, "Plaintiffs"), individually and on behalf of all similarly situated financial institutions (the "Class Members"), complain of the actions of Defendant Schnuck Markets, Inc. ("Schnucks"), and respectfully state the following:

NATURE OF THE CASE

1. This is a data breach case. Plaintiffs' Complaint rests on multiple violations of the federal wire fraud and bank fraud statutes prohibiting "schemes to defraud" where the fraud is "representational" and where the fraud amounts to "cheating" without representations. This Complaint alleges violations of the federal wire fraud and bank fraud statutes in both ways. Plaintiffs also allege multiple common law causes of action and statutory violations.

2. Schnucks is a grocery chain in the upper Midwest. Plaintiffs and Class Members are financial institutions that issued approximately 2.4 million credit cards and debit cards (together, "payment cards") that were fraudulently compromised by a data breach within Schnucks' internal computer systems (the "Schnucks Data Breach" or "Data Breach" or "Breach"), from December 2012 through March 30, 2013. As a direct and proximate result of Schnucks' wrongful actions, inaction, and omissions, and the resulting Data Breach, Plaintiffs and Class Members have incurred (and will continue to incur) damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

3. As part and parcel of the Schnucks Data Breach, hackers targeted specific vulnerabilities in Schnucks' computer systems, hijacking confidential and sensitive unencrypted payment card information from Schnucks' "processing environment" within its internal computer systems while the 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 and sensitive payment card information and other customer data at approximately 79 of the 100 Schnucks retail locations in Missouri, Illinois, Indiana, and Wisconsin. The malware "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.

4. The wrongfully disclosed and compromised payment card information was sold by illicit websites as "dumps" to international card counterfeiters, fraudsters, and issuing financial institutions attempting to mitigate their risk. Crooks create counterfeit credit cards by encoding the payment card information onto any card with a magnetic stripe, and use the counterfeit cards to make fraudulent purchases. Fraudsters also create fake debit cards with the payment card information, and then use the counterfeit cards to make fraudulent purchases and withdraw cash from the bank accounts of unsuspecting victims through ATMs. Confirmed fraud involving the wrongfully disclosed and compromised 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.

5. The Schnucks Data Breach could have, and should have, been prevented if Schnucks had been in compliance with the Visa Operating Regulations, the MasterCard Rules,

Payment Card Industry Data Security Standards ("PCI DSS"),[1] and Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.[2]

6. At all relevant times, Plaintiffs and Class Members were (and continue to be) members of the Visa and MasterCard Networks. Since at least December 2012, (and possibly earlier), Schnucks engaged in unlawful and intentional schemes to (i) defraud Plaintiffs and Class Members via intentional misrepresentations and omissions (on which they justifiably relied), and (ii) defraud Plaintiffs and Class Members by cheating them—both in an effort to obtain money, funds, credits, assets, and other property owned by, or under the custody or control of, Plaintiffs and Class Members.

7. The "representational" scheme to defraud involved means of false or fraudulent pretenses and fraudulently and intentionally misrepresenting to Plaintiffs and Class Members—explicitly and implicitly—through millions of electronic payment card transactions for which Schnucks sought authorization from Plaintiffs and Class Members via the interstate wires, its website, and its participation in the Visa Network and MasterCard Network that (a) Schnucks was in compliance with the Visa Operating Regulations and MasterCard Rules mandating the protection of payment card information, (b) Schnucks was in compliance with the PCI DSS, (c) Schnucks was not committing unlawful, unfair and deceptive acts or practices, in violation of Section 5 of the FTC Act, by failing to implement, monitor, and maintain the proper customer

[1] www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0 (last visited January 13, 2015).

[2] As interpreted and enforced by the FTC, Schnucks' failure to implement, monitor, and maintain the proper customer data security policies, procedures, protocols, and hardware and software systems to safeguard and protect the confidential and sensitive payment card information and other customer data compromised in the Data Breach, as well as the related above-described schemes to cheat and defraud Plaintiffs and Class Members, collectively constitute 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).

data security policies, procedures, protocols, and hardware and software systems to safeguard and protect the confidential and sensitive payment card information and other customer data compromised in the Data Breach, and (d) Schnucks' customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect confidential and sensitive payment card information and other customer data—including the wrongfully disclosed and compromised payment card information—for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Schnucks and approve millions of electronic payment card transactions at Schnucks via the interstate wires for the further purpose of increasing Schnucks' revenue, profitability, and return on investment. Alternatively, Schnucks fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true.

8. Plaintiffs and Class Members justifiably relied on Schnucks' intentional misrepresentations, and omissions, and issued payment cards used to make purchases at Schnucks and approved millions of electronic payment card transactions at Schnucks. Had Plaintiffs and Class Members known Schnucks' representations and omissions were false, they would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the confidential and sensitive payment card information and other customer data themselves.

9. Schnucks' above-described wrongful actions, inaction, and omissions also operated as a "cheating" scheme to defraud; to wit, Plaintiffs and Class Members were cheated in their business and property as a direct, proximate, and intended result of Schnucks' above-described wrongful actions, inaction, and omissions.

10. By engaging in these unlawful and intentional schemes, (i) Plaintiffs and Class Members suffered the above-described damages to their businesses and property, and other

actual injury and harm, (ii) Schnucks saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (iii) Schnucks wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members. Schnucks intentionally engaged in these wrongful actions, inaction, and omissions for its financial benefit, and Plaintiffs' and Class Members' financial detriment.

11. Plaintiffs, for themselves and Class Members, bring this action against Schnucks as a national class action under Title XI of Public Law 91-452, 84 Stat. 922 (1970) (as codified at 18 U.S.C. §§ 1961–1968, as amended) for engaging in the above-described intentional schemes and unlawful conduct. At all relevant times, by its wrongful actions, inaction, and omissions, Schnucks conducted and participated, directly and indirectly, in the affairs of the Visa Network and MasterCard Network (the enterprises) through a pattern of wrongful activity—to wit, Schnucks engaged in repetitious and systematic interstate wire fraud, in violation of 18 U.S.C. § 1343, and bank fraud, in violation of 18 U.S.C. § 1344, by using or causing the use of the wires in interstate commerce to intentionally, repeatedly and systematically devise, engage in, condone, and ratify the above-described schemes to defraud Plaintiffs and Class Members—all of which are financial institutions—(i) by making intentional misrepresentations or omissions to Plaintiffs and Class Members (on which they justifiably relied), and (ii) by cheating Plaintiffs and Class Members to obtain money, funds, credits, assets, and other property owned by, or under the custody or control of, Plaintiffs and Class Members.

12. Schnucks' wrongful actions, inaction, and omissions, as it well knew and intended, and without legal justification, (i) unlawfully cheated Plaintiffs and Class Members out of money, funds, credits, assets, and other property owned by, or under the custody or control of, Plaintiffs and Class Members, and (ii) induced Plaintiffs and Class Members to issue payment cards used to make purchases at Schnucks and approve millions of electronic payment card

transactions at Schnucks via the interstate wires knowing that its customer data security policies, procedures, protocols, and hardware and software systems, in fact, did not safeguard and protect confidential and confidential and sensitive customer data—including the wrongfully disclosed and compromised payment card information and other customer data.

13. At all relevant times, by its wrongful actions, inaction, and omissions, Schnucks (i) conducted or participated in the affairs of the Visa and MasterCard Networks (the enterprises) (in violation of 18 U.S.C. § 1962(c)), and (ii) conspired to violate 18 U.S.C. § 1962(a) and (c) (in violation of 18 U.S.C. § 1962(d)).

14. Schnucks agreed to commit (and committed) these substantive offenses (*i.e.*, the above-described unlawful and intentional schemes through the enterprises (*i.e.*, the Visa Network and MasterCard Network)) by engaging in multiple predicate acts of interstate wire fraud and bank fraud—all the while knowing of, and intentionally agreeing to, the overall objective of the schemes knowing that its customer data security policies, procedures, protocols, and hardware and software systems, in fact, did not safeguard and protect confidential and sensitive customer data, including the wrongfully disclosed and compromised confidential and sensitive payment card information and other customer data—thereby damaging Plaintiffs' and Class Members' businesses and property, and inflicting other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

15. Schnucks knew, and intentionally so acted, that Plaintiffs and Class Members are part of the Visa and MasterCard Networks and rely on merchants that accept Visa and

MasterCard payment cards to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems across its computer systems. Schnucks also knew, and intentionally so acted, that its above-described wrongful actions, inaction, and omissions were fraudulent, misleading and unlawful, and would unlawfully cheat and defraud Plaintiffs and Class Members in their businesses and property, and take unlawful and unfair advantage of Plaintiffs and Class Members.

16. Schnucks' above-described unlawful and intentional schemes, wrongful actions, inaction, and omissions, and the resulting Data Breach also constitute breach of fiduciary duty, negligence/gross negligence, negligence *per se*, negligent misrepresentation, breach of 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, unjust enrichment/assumpsit, and equitable subrogation.

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

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over Plaintiffs' claims under (i) 18 U.S.C. § 1961, *et seq.*, pursuant to 18 U.S.C. § 1964(a);(c); (ii) 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 (iii) 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.

19. 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) and 18 U.S.C § 1965.

PARTIES

20. Plaintiff Community Bank of Trenton ("CBT") is an Illinois financial institution with its principal place of business in Trenton, Illinois. CBT issued payment cards compromised by the Schnucks Data Breach. As a direct and proximate result of Schnucks' above-described unlawful and intentional schemes to defraud involving intentional misrepresentations and cheating, wrongful actions, inaction, and omissions (on which CBT justifiably relied), CBT has incurred (and will continue to incur) damages to its business and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Had CBT known Schnucks' representations and omissions were false, it would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the compromised confidential and sensitive payment card information and other customer data

itself.

21. Plaintiff University of Illinois Employees Credit Union ("UIECU") is an Illinois financial institution with its principal place of business in Champaign, Illinois. UIECU issued payment cards compromised by the Schnucks Data Breach. As a direct and proximate result of Schnucks' above-described unlawful and intentional schemes to defraud involving intentional misrepresentations and cheating, wrongful actions, inaction and omissions (on which UIECU justifiably relied), UIECU has incurred (and will continue to incur) damages to its business and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Had UIECU known Schnucks' representations and omissions were false, it would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the compromised confidential and sensitive payment card information and other customer data itself.

22. Plaintiff First Federal Savings Bank of Champaign-Urbana ("FFSB") is an Illinois financial institution with its principal place of business in Champaign, Illinois. FFSB issued payment cards compromised by the Schnucks Data Breach. As a direct and proximate result of Schnucks' above-described unlawful and intentional schemes to defraud involving intentional misrepresentations and cheating, wrongful actions, inaction, and omissions (on which FFSB justifiably relied), FFSB has incurred (and will continue to incur) damages to its business and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Had FFSB known Schnucks' representations and omissions were false, it would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the compromised confidential and sensitive payment card information and other customer data itself.

23. Plaintiff Southpointe Credit Union ("SPCU") is a Missouri financial institution with its principal place of business in St. Louis, Missouri. SPCU issued payment cards compromised by the Schnucks Data Breach. As a direct and proximate result of Schnucks' above-described unlawful and intentional schemes to defraud involving intentional misrepresentations and cheating, wrongful actions, inaction, and omissions (on which Southpointe justifiably relied), SPCU has incurred (and will continue to incur) damages to its business and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Had SPCU known Schnucks' representations and omissions were false, it would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the compromised confidential and sensitive payment card information and other customer data itself.

24. Defendant Schnuck Markets, Inc. ("Schnucks") is a Missouri corporation headquartered in St. Louis, Missouri. Schnucks owns and operates approximately 100 retail

supermarkets in Missouri, Indiana, Wisconsin, Iowa, and Illinois—including the Southern District of Illinois. Schnucks also 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 their authorization for electronic payment card transactions.

25. At all relevant times, Schnucks engaged in the above-described unlawful and intentional schemes to defraud involving intentional misrepresentations and cheating, wrongful actions, inaction, and omissions (on which Plaintiffs and Class members justifiably relied) that directly and proximately caused Plaintiffs and Class Members to suffer damages to their business and property 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Schnucks engaged in the above-described unlawful and intentional schemes to defraud, wrongful actions, inaction, and omissions for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Schnucks and approve electronic payment card transactions at Schnucks via the interstate wires for the further purpose of increasing Schnucks' revenue, profitability, and return on investment. Schnucks may be served with Summons and a copy of this Class Action Complaint and Jury Demand by serving its registered agent for service of process, National Registered Agents, Inc., 200 West Adams Street, Chicago, Illinois 60606.

FACTS

I. Payment card transactions on the Visa and MasterCard Networks.

26. The Visa and MasterCard Networks are principally composed of acquiring banks (*i.e.*, financial institutions that contract with merchants to process their Visa and MasterCard payment card transactions) and payment card issuers (such as Plaintiffs and Class Members).

27. A typical payment card transaction made on the Visa and MasterCard Networks has multiple moving parts handled by several different parties. A transaction is initiated by a merchant (here, Schnucks), electronically sent to its acquiring bank (here, Citicorp), processed by a payment card transaction processor (*i.e.*, an entity retained by the acquiring bank to actually process the transaction) (here, First Data Merchant Services Corp. ("First Data")), and authorized by the payment card issuer (here, Plaintiffs and Class Members).

28. When a payment card purchase is made on the Visa Network,[3] the merchant seeks authorization from the issuer, which approves or declines the transaction based on the consumer's payment card limit. If the transaction is approved, the merchant processes the transaction and electronically forwards the receipt directly to the acquiring bank. The acquiring bank then pays the merchant, and forwards the final transaction data to the issuer which, in turn, reimburses the acquiring bank. The issuer then posts the charge to the consumer's payment card account, and bills and collects the purchase price from the consumer.

29. In accordance with their respective regulations and operating procedures, Visa and MasterCard monitor their respective Networks for fraudulent activity. When fraudulent payment card use is suspected, MasterCard notifies affected issuers through a Security Alert

[3] Transactions made on the MasterCard Network are identical in all relevant respects. The only substantive difference is that in the MasterCard Network, the merchant initially seeks authorization/verification from its acquiring bank, which seeks reimbursement from the issuer.

while Visa notifies affected issuers via a "Compromised Account Management Systems Alert," or "CAMS Alert." These alerts generally set forth the type of compromised data, the relevant timeframe of the compromise, and a list of payment card numbers that have been exposed.

30. Schnucks accepts payment cards in payment for its customers' purchases. When a consumer makes a payment card purchase at a Schnucks supermarket, Schnucks collects confidential and sensitive payment card information and other customer data, including the cardholder's name, account number, expiration date, CVV codes (security codes), and PIN numbers for debit cards (collectively, "track data") stored on the magnetic strip of the swiped payment card. 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 transaction for payment. Schnucks also collects and stores other consumer data, including mailing addresses, phone numbers, and email addresses.

31. 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.

II. Prior to the Data Breach, Schnucks knew its computer systems were not properly protected or compliant with the PCI DSS, Visa Operating Regulations, and MasterCard Rules.

32. Prior to the Data Breach, Schnucks knew full well its data security policies, procedures and protocols were inadequate, yet did nothing to upgrade and improve such policies, procedures and protocols in the name of cost savings and avoiding the perceived disruption in business. Schnucks also knew it was not compliant with the Visa Operating Regulations, MasterCard Rules, and PCI DSS.

33. The PCI DSS is the industry standard for retail institutions that accept payment cards. The PCI DSS consists of twelve general standards for (i) installing and maintaining firewall(s) to protect data, (ii) protecting stored data, (iii) encrypting the transmission of

confidential and sensitive payment card information and other customer data across public networks, (iv) using and regularly updating antivirus software, (v) developing and maintaining secure systems and applications, (vi) restricting physical access to cardholder data, (vii) tracking and monitoring all access to network resources and cardholder data, (viii) regularly testing security systems and processes, and (ix) maintaining policies addressing information security.

34. The purpose of the PCI DSS is to "[b]uild and maintain a secure network; protect cardholder data; ensure the maintenance of vulnerability management programs; implement strong access control measures; regularly monitor and test networks; and ensure the maintenance of information security policies." *See* www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

35. Under the PCI DSS, merchants like Schnucks are required to encrypt "track data." The Data Breach never should have happened. The fact that track data was compromised shows it was being improperly stored. Storing track data has long been banned by Visa, MasterCard, and the PCI Security Standards Council.

36. To comply with the PCI DSS, a merchant must:

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

(emphasis in original).[4]

37. PCI compliance also requires retailers to "install firewalls and forbid using pass

[4] *How to Be Compliant: Getting Started with PCI Data Security Standard Compliance*, PCI SSC, available at ttps://www.pcisecuritystandards.org/merchants/how_to_be_compliant.php (last visited January 13, 2015).

codes that come with applications . . . [and] how credit card data should be stored."[5]

38. Schnucks knowingly failed to adequately analyze its computer systems containing payment card data, and knowingly failed to fix vulnerabilities in its computer systems—which directly and proximately resulted in the Data Breach.

39. Schnucks admits it is a "Level 1" merchant—in that it processes more than 6 million card transactions a year—which requires it "to undergo quarterly network scans and an annual audit."[6] Yet, Schnucks knowingly or recklessly did not compile and submit remediation and validation records and compliance reports to Citicorp, its acquiring bank, Visa, and MasterCard.

40. 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.

Id.

41. Despite these restrictions, Schnucks knowingly permitted or recklessly allowed the account numbers and expiration dates (and possibly more information and data) for payment cards issued by Plaintiffs and Class Members to be wrongfully disclosed and compromised.

42. The hackers could not have targeted and accessed Schnucks' internal computer systems, and obtained Plaintiffs' and Class Members' confidential and sensitive payment card information and other customer data, but for Schnucks' knowing or reckless inadequate

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

[6] *Id.*

cybersecurity—including its failure to comply with the Visa Operating Regulations, MasterCard Rules, and PCI DSS. Schnucks knowingly or recklessly failed to implement and maintain appropriate customer data security policies, procedures, protocols, and hardware and software systems to safeguard and protect the nature and scope of the payment card information wrongfully disclosed and compromised in the Data Breach.

III. The Schnucks Data Breach.

43. According to Schnucks, on or about March 14, 2013, it first learned of the Data Breach when its payment card processor alerted it to fraud on a handful of payment cards that had been recently used at Schnucks stores. Schnucks allegedly launched an internal investigation, ruling out insider theft and point-of-sale devices as potential causes.

44. On or about March 19, 2013, Schnucks hired cybersecurity firm Mandiant to investigate further amid reports of more fraud. Even then, Schnucks did not isolate and shut down the Data Breach until March 28, 2013. Thereafter, it took another 36 hours to contain the Data Breach, and bolster security to prevent a recurrence.

45. According to Schnucks, the compromised payment card information was obtained from the payment card "processing environment" in its internal computer systems while the payment card transactions were awaiting approval. The fraudsters supposedly accessed the information by inserting malware into Schnucks' computer systems. The confidential and sensitive payment card information and other customer data was lifted shortly after the payment cards were swiped at the point of sale.

46. According to Al Pascual, a senior analyst of security risk and fraud at Javelin Strategy & Research, a California company that advises the payment industry, "[t]he Schnucks

breach was the result of random access memory malware."[7] "That means there's malicious software at the point of sale. After a card is swiped, the data goes into the register, then it goes to random access memory on the computer itself, and this malware pulls it right off the memory before it is transmitted somewhere else." Thus, the compromised payment card information was taken as it moved through Schnucks' internal computer systems. Because the compromised information was not encrypted, the fraudsters had complete access to it, and use of it.

47. Merchants—such as Schnucks—that choose their payment card processor based on the lowest price typically are victims of these types of data breaches. Encrypting the payment card data at the reader, rather than in the point of sale, all but eliminates the ability for "skimming" devices or malware to be used because the payment card data is encrypted before it reaches the computer or cables connecting the computers to the reader. Schnucks knowingly or recklessly chose its payment card processor, heedlessly in disregard of the best interests of Plaintiffs and Class Members, based on the lowest price, and not the highest quality of cybersecurity delivered.

48. The Data Breach compromised payment cards issued by Plaintiffs and Class Members for purchases made between December 2012 and March 30, 2013, demonstrating that Schnucks knowingly failed and refused to safeguard and protect Plaintiffs' and Class Members' payment card information between the time it was first alerted about the Data Breach and the time it claims the Data Breach was contained.

49. On March 30, 2013—two weeks after it learned about the Data Breach—Schnucks issued a press release stating that its computer systems had been compromised. Schnucks revealed that hackers had targeted and implanted malicious computer code into its

[7] Georgina Gustin, *Crooks Who Stole Schnucks Data Lie Far from Law Enforcement's Grasp*, stltoday.com, available at http://www.stltoday.com/business/local/crooks-who-stole-Schnuckss-data-lie-far-from-law-enforcement/article_300e2f15-ff72-5dbe-9efd-211aa91817f6.html (last visited January 13, 2015).

computer systems that captured payment card numbers and expiration dates (and possibly more information and data).

50. Schnucks further acknowledged that even though it contained the Breach, any payment card that was already accessed could still experience fraud—meaning that Plaintiffs and Class Members are at an ongoing and continuing risk of fraudulent purchases on compromised payment cards that have not yet been replaced.

51. At the time of the Data Breach, Schnucks knowingly or recklessly was not in compliance with the Visa Operating Regulations, MasterCard Rules, and PCI DSS.

52. Although Schnucks' failure to comply with the Visa Operating Regulations, MasterCard Rules, and PCI DSS provided it with short-term and fleeting benefits in the form of the cost savings of compliance, such savings were to the financial detriment of 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 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

IV. The Schnucks Data Breach never should have happened.

53. The Schnucks Data Breach never should have happened. Schnucks knew or recklessly risked that its data security policies, procedures, protocols, and hardware and software systems were insufficient, antiquated, and did not safeguard and protect confidential and sensitive payment card information and other customer data from theft, yet did nothing to expand, improve, or update them.

54. In addition to bringing its internal computer network into compliance with PCI DSS, the Data Breach 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. Even for an entity the size of Schnucks, a fully developed ERM system would have cost Schnucks a fraction of the estimated cost of the Schnucks Data Breach.[8] Schnucks, however, knowingly or recklessly failed and refused to develop and implement an effective ERM system.

55. The Data Breach also would have been prevented had Schnucks installed the appropriate antivirus software across its entire internal systems. Several readily available antivirus software programs—such as AVG, Bitdefender and ThreatTrack—would have detected and removed the malware used by the hackers. Schnucks, however, knowingly or recklessly failed or refused to install the appropriate antivirus software across its computer systems.

56. The Data Breach also would have been prevented had Schnucks properly monitored its computer networks for signs of attack. Schnucks, however, knowingly or recklessly failed and refused to do so.

57. The key to effective data security is layered security—which Schnucks did not have in place. Had layered data security been in place, the fraudsters would have first had to determine how to deploy the malware, and then determine how to circumvent the antivirus software running on the computer network. Even if they could have accomplished these feats—

[8] According to the Ponemon Institute, a data breach costs U.S. companies an average of $188 per compromised customer record. *See 2013 Cost of a Data Breach Study, United States*, PONEMON INSTITUTE, June 13, 2013.

which would not have been possible—the malware would have been blocked by the firewall or network segmentation when attempting to access the Internet. Had Schnucks taken even the most fundamental layered data security measures, the Data Breach never would have happened.

58. While Schnucks threw consumers somewhat of a bone in an effort to rebuild customer loyalty and improve its financial outlook, it has not offered Plaintiffs and Class Members any compensation for the hard damages they have suffered (and will continue to suffer). This suit has resulted.

SCHNUCKS' PATTERN OF UNLAWFUL ACTIVITY UNDER 18 U.S.C. § 1961, *et seq.*: INTERSTATE WIRE FRAUD AND BANK FRAUD

59. The preceding factual statements and allegations are incorporated by reference.

60. Schnucks knew, and intentionally so acted, that Plaintiffs and Class Members are financial institutions and members of the Visa and MasterCard Networks that rely on merchants accepting Visa and MasterCard payment cards to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems across their internal computer systems compliant with the standards set forth in the Visa Operating Regulations, MasterCard Rules, and PCI DSS. The Visa Operating Regulations, MasterCard Rules, and PCI DSS data security standards are designed to provide the maximum security possible for confidential and sensitive payment card information and other customer data.

61. Schnucks, however, intentionally (i) "gamed" the Visa and MasterCard Networks, (ii) disregarded the Visa Operating Regulations, MasterCard Rules, and PCI DSS data security standards, (iii) managed and operated the Visa and MasterCard Networks by unilaterally devising, implementing, and imposing its own non-compliant customer data security policies, procedures, protocols, and hardware and software systems that did not provide such a high level of data protection, (iv) saved the cost of implementing the proper customer data security policies,

procedures, protocols, and hardware and software systems, and (v) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members.

62. Schnucks then devised, engaged in, condoned, and ratified the above-described open-ended and unlawful "representational" and "cheating" schemes to (i) cheat and defraud Plaintiffs and Class Members to obtain money, funds, credits, assets, and other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or fraudulent pretenses, and (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate wires, its website, and its participation in the Visa and MasterCard Networks that (a) it was in compliance with the Visa Operating Regulations and MasterCard Rules mandating the protection of payment card information, (b) it was in compliance with the PCI DSS, (c) Schnucks was not committing unlawful, unfair and deceptive acts or practices, in violation of Section 5 of the FTC Act, by failing to implement, monitor, and maintain the proper customer data security policies, procedures, protocols, and hardware and software systems to safeguard and protect the confidential and sensitive payment card information and other customer data compromised in the Data Breach, and (d) its customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect confidential and sensitive payment card information and other customer data—including the wrongfully disclosed and compromised payment card information—both for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Schnucks and approve millions of payment card purchases made at Schnucks via the interstate wires for the further purpose of increasing Schnucks' revenue, profitability, and return on investment. Alternatively, Schnucks fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse

was true.

63. Plaintiffs and Class Members justifiably relied on Schnucks' intentional misrepresentations and omissions, issued payment cards used to make purchases at Schnucks, and approved millions of payment card purchases made at Schnucks. By doing so, (i) Plaintiffs and Class Members suffered damages to their businesses and property, (ii) Schnucks saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (iii) Schnucks wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members. Schnucks intentionally engaged in these wrongful actions, inaction, and omissions for its financial benefit and to Plaintiffs' and Class Members' financial detriment. Had Plaintiffs and Class Members known such representations and omissions were false, they would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the compromised confidential and sensitive payment card information and other customer data themselves.

64. Schnucks' above-described unlawful and intentional schemes, wrongful actions, inaction, and omissions wrongfully cheated Plaintiffs and Class Members, and violated all concepts of moral uprightness, fundamental honesty, fair play, and right dealing in the general and business life of the members of society. Schnucks' above-described unlawful and intentional schemes, wrongful actions, inaction, and omissions also unfairly betrayed the confidences Plaintiffs and Class Members placed in Schnucks. Schnucks' above-described unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions also were a consistent, regular and dominant part of the manner in which it participated in, and conducted its day-to-day business dealings with Plaintiffs and Class Members.

65. Schnucks intentionally devised, instigated, perpetrated, executed, condoned, and ratified the above-described schemes to cheat and defraud by engaging in the above-described

repeated and systematic interstate wire fraud and bank fraud by using and causing the use of the interstate wires to (i) secure the authorization of millions of payment card transactions from Plaintiffs and Class Members, each being a separate violation of 18 U.S.C. §§ 1343 and 1344, and (ii) post to and maintain its website, and participate in the Visa and MasterCard Networks, each also being a separate violation of 18 U.S.C. §§ 1343 and 1344.

66. Schnucks managed and operated the Visa and MasterCard Networks (the enterprises) in such a way as to use the interstate wires in interstate commerce to devise, engage in, condone, and ratify the above-described open-ended, unlawful and intentional schemes to cheat and defraud by means of false or fraudulent pretenses, intentional misrepresentations, and false promises (on which Plaintiffs and Class Members justifiably relied) through millions of electronic payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate wires, its website, and its participation in the Visa and MasterCard Networks, without the knowledge or approval of Plaintiffs and Class Members, for the purposes of increasing Schnucks' revenue, profitability, and return on investment. The dates and substance of Schnucks' internal and external fraudulent communications, via the interstate wires, in furtherance of the above-described schemes, as well as its fraudulent communications to Plaintiffs and Class Members, via the interstate wires, in furtherance of such schemes to cheat and defraud, are in Schnucks' possession, custody, and control, and await discovery.

67. Had Plaintiffs and Class Members known such representations and omissions were false, they would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the compromised confidential and sensitive payment card information and other customer data themselves. By its unlawful actions, inaction, and omissions, Schnucks (i) conducted or participated in the affairs of the Visa Network and MasterCard Network (the enterprises) (in violation of 18 U.S.C. § 1962(c)), and (ii) conspired to

violate 18 U.S.C. § 1962 (a) and (c) (in violation of 18 U.S.C. § 1962(d)), cheating and defrauding Plaintiffs and Class Members in the process.

68. Schnucks managed and operated the Visa and MasterCard Networks in such a way as to engage in the above-described open-ended, unlawful, intentional and fraudulent schemes to cheat and defraud—without Plaintiffs' and Class Members' knowledge or approval—for the purpose of increasing Schnucks' revenue, profitability, and return on investment to their financial detriment. Schnucks' above-described unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions constitute interstate wire fraud, in violation of 18 U.S.C. § 1343, and bank fraud, in violation of 18 U.S.C. § 1344.

69. Schnucks' above-described multiple, repeated and continuous acts of interstate wire fraud and bank fraud constitute a pattern of unlawful activity under to 18 U.S.C. § 1961(1); (5). Nothing in the nature of the open-ended, unlawful, intentional and fraudulent schemes demonstrates that Schnucks' unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions would ever have terminated but for this Court's intervention. Moreover, and independent of the duration of the schemes, Schnucks' above-described unlawful and intentional schemes, wrongful actions, inaction, and omissions were a consistent, regular and dominant part of the manner in which it conducted or participated in the day-to-day business and financial affairs of the Visa and MasterCard Networks.

CLASS ACTION ALLEGATIONS

70. 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, 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) absorbed unauthorized

charges made on the compromised payment cards.

71. 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 classes of similarly situated payment card issuers (together, the "State Sub-Classes"):

> **ILLINOIS.** All 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) absorbed unauthorized charges made on the compromised payment cards (the "Illinois Sub-Class").
>
> **MISSOURI.** All 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) absorbed unauthorized charges made on the compromised payment cards (the "Missouri Sub-Class").

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

73. 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, which Schnucks, Visa, or MasterCard have already notified about the Breach.

74. Schnucks violated the rights of each Class Member in the same way by its above-described uniform unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions.

75. 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 unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions violated 18 U.S.C. § 1962(c) and (d);

(ii) whether Schnucks' above-described wrongful actions, inaction, and omissions constitute breach of fiduciary duty at common law;

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

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

(v) whether Schnucks' above-described wrongful actions, inaction, and omissions constitute negligent misrepresentation at common law;

(vi) whether Schnucks' above-described unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions constitute breach of implied contract at common law;

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

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

(ix) 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;

(x) whether Schnucks should be compelled to refund (or disgorge) the amounts by which it has been unjustly enriched under the common law doctrine of equitable subrogation;

(xi) whether Schnucks' above-described unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions directly or proximately caused Plaintiff and Class Members to suffer damages;

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

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

76. Plaintiffs' claims are typical of Class Members' claims because Plaintiffs and Class Members are all victims of Schnucks' above-described schemes to cheat and defraud by means of false or fraudulent pretenses, intentional misrepresentations, false promises, omissions, or otherwise unlawful conduct.

77. 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, financial institution cases, and cases asserting violations of 18 U.S.C. §§ 1961–1968.

78. 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 unlawful and intentional schemes, 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.

79. Class Members are readily ascertainable since they have all been notified that payment cards issued by them were compromised by the Data Breach, whereupon they cancelled and re-issued such compromised payment cards, absorbed fraudulent charges made on the compromised payment cards, or both.

80. 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.

81. 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.

82. 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.

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

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

CLAIMS FOR RELIEF/ CAUSES OF ACTION

COUNT I

VIOLATIONS OF 18 U.S.C. § 1962(c)
(On behalf of the Nationwide Class and State Sub-Classes)

85. The preceding factual statements and allegations are incorporated by reference.

86. Each Plaintiff and each Class Member is a "person" within the meaning of 18 U.S.C. §§ 1961(3), 1964(c). Each Plaintiff and each Class Member also is a "financial institution" within the meaning of 18 U.S.C. § 1344.

87. Schnucks is a "person" within the meaning of 18 U.S.C. §§ 1961(3) and 1962(a).

88. The Visa and MasterCard Networks each are "enterprises" within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c) and, at all relevant times, were engaged in, and the activities of which affected, interstate commerce within the meaning of 18 U.S.C. §§ 1961(4), 1962(c), 1962(d).

89. Schnucks conducted and participated in the business and financial affairs of the Visa and MasterCard Networks (the enterprises) through a pattern of unlawful activity within the meaning of 18 U.S.C. §§ 1961(1)(B), 1961(5), 1962(c)—to wit, Schnucks managed and operated the Visa and MasterCard Networks by intentionally devising and implementing its own non-compliant customer data security policies, procedures, protocols, and hardware and software systems (as described above), and then devised, engaged in, condoned, and ratified the above-described open-ended and unlawful "representational" and "cheating" schemes to (i) cheat and defraud Plaintiffs and Class Members to obtain money, funds, credits, assets, and other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or fraudulent pretenses, and (ii) fraudulently and intentionally misrepresent to Plaintiffs and Class Members—explicitly and implicitly—through millions of payment card purchases for which it sought authorization from Plaintiffs and Class Members via the interstate wires, its website, and its participation in the Visa and MasterCard Networks that (a) it was in compliance with the Visa Operating Regulations and MasterCard Rules mandating the protection of payment card information, (b) it was in compliance with the PCI DSS, (c) Schnucks was not committing unlawful, unfair and deceptive acts or practices, in violation of Section 5 of the FTC Act, by

failing to implement, monitor, and maintain the proper customer data security policies, procedures, protocols, and hardware and software systems to safeguard and protect the confidential and sensitive payment card information and other customer data compromised in the Data Breach, and (d) its customer data security policies, procedures, protocols, and hardware and software systems were in place and would safeguard and protect confidential and sensitive payment card information and other customer data—including the wrongfully disclosed and compromised payment card information—both for the purpose of inducing Plaintiffs and Class Members to issue payment cards used to make purchases at Schnucks and approve millions of electronic payment card purchases made at Schnucks, via the interstate wires, for the further purpose of increasing Schnucks' revenue, profitability, and return on investment. Alternatively, Schnucks fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true.

90. Plaintiffs and Class Members justifiably relied on Schnucks' intentional misrepresentations and issued payment cards used to make purchases at Schnucks and approved millions of electronic payment card transactions at Schnucks to their financial detriment. Had Plaintiffs and Class Members known such representations and omissions were false, they would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the compromised payment card information and confidential and sensitive payment card information and other customer data themselves The above-described multiple, repeated, and continuous acts of interstate wire fraud and bank fraud violated 18 U.S.C. §§ 1343 and 1344.

91. Schnucks' pattern of unlawful activity and corresponding violations of 18 U.S.C. § 1962(c) directly and proximately caused Plaintiffs and Class Members to suffer injury to their businesses and property within the meaning of 18 U.S.C. § 1964(c)—to wit, Plaintiffs and Class Members were damaged (and will continue to be damaged) by Schnucks' above-described

repeated and systematic interstate wire fraud and bank fraud, in violation of 18 U.S.C. §§ 1343 and 1344, to devise, engage in, condone, and ratify the above-described open-ended, unlawful and intentional schemes to cheat and defraud Plaintiffs and Class Members to obtain money, funds, credits, assets, and other property owned by, or under the custody or control of, Plaintiffs and Class Members. Plaintiffs and Class Members have suffered (and will continue to suffer) damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Schnucks also (i) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (ii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members. Schnucks' conduct also constituted a cheat in violation of 18 U.S.C. §§ 1343 and 1344.

92. As described above, Schnucks intentionally managed and operated the Visa and MasterCard Networks (the enterprises) in such a way as to engage in multiple predicate acts of interstate wire fraud and bank fraud to, in turn, engage in the above-described open-ended, unlawful, intentional and fraudulent schemes by means of false or fraudulent pretenses, intentional misrepresentations, or false promises (on which Plaintiffs and Class Members justifiably relied)—for the purpose of increasing Schnucks' revenue, profitability, and return on investment to the financial detriment of Plaintiffs and Class Members.

93. Schnucks knew or recklessly should have known its above-described unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions were

fraudulent, misleading and illegal, and would cause Plaintiffs and Class Members to suffer the above-described damages in their business and property within 18 U.S.C. §1964(c). All of Plaintiffs' and Class Members' damages were reasonably foreseeable by Schnucks and anticipated as a substantial factor and a natural consequence of its pattern of unlawful activity.

COUNT II

VIOLATION OF 18 U.S.C. § 1962(d) BY CONSPIRING TO VIOLATE 18 U.S.C. § 1962(a)
(On behalf of the Nationwide Class and State Sub-Classes)

94. The preceding factual statements and allegations are incorporated by reference.

95. Each Plaintiff and each Class Member is a "person" within the meaning of 18 U.S.C. §§ 1961(3), 1964(c). Each Plaintiff and each Class Member also is a "financial institution" within the meaning of 18 U.S.C. § 1344.

96. Schnucks is a "person" within the meaning of 18 U.S.C. §§ 1961(3) and 1962(a).

97. Schnucks also is an "enterprise" within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c) and, at all relevant times, was engaged in, and the activities of which affected, interstate commerce within the meaning of 18 U.S.C. §§ 1961(4), 1962(c), 1962(d).

98. Schnucks conspired with other persons and entities, the identities of whom are known only to Schnucks at this time and await discovery, within the meaning of 18 U.S.C. § 1962(d), to violate 18 U.S.C. § 1962(a); that is, Schnucks and its co-conspirators conspired to receive income derived, directly or indirectly, from a pattern of unlawful activity in which Schnucks and its co-conspirators participated as principals within the meaning of 18 U.S.C. §§ 1961(1)(B), 1961(5), and 1962(a)—to wit, the above-described open-ended, unlawful and fraudulent schemes to manage and operate the Visa and MasterCard Networks, and cheat and defraud Plaintiffs and Class Members to obtain money, funds, credits, assets, and other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or

fraudulent pretenses and intentional misrepresentations. Alternatively, Schnucks fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true.

99. As a direct and proximate result of Schnucks' above-described multiple and repeated acts of interstate wire fraud and bank fraud, Plaintiffs and Class Members have suffered (and will continue to suffer) damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Schnucks also (i) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (ii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members.

100. Schnucks and its co-conspirators intentionally participated in a conspiracy to engage in the above-described interstate wire fraud, bank fraud, unlawful and intentional schemes, wrongful actions, inaction, and omissions for Schnucks' financial benefit and to Plaintiffs' and Class Members' financial detriment in violation of 18 U.S.C. §§ 1343 and 1344. The members, time and place of this complex, multi-party conspiracy are known only by Schnucks at this time and await discovery.

101. Schnucks used or invested (and continues to use or invest), directly or indirectly, such income, or the proceeds of such income, in its ongoing participation in the Visa and MasterCard Networks (the enterprises) and the creation and operation of one or more other Schnucks-owned stand-alone enterprises (known only by Schnucks at this time), all of which are engaged in, or the activities of which affect, interstate commerce.

102. As described above, Schnucks and its co-conspirators managed and operated the Visa and MasterCard Networks (the enterprises) in such a way as to engage in the above-described multiple predicate acts of interstate wire fraud and bank fraud for the purpose of increasing Schnucks' profitability and return on investment to Plaintiffs' and Class Members' financial detriment.

103. Schnucks knew, or recklessly should have known, its unlawful and intentional conspiracy and commission of the above-described interstate wire fraud, bank fraud, wrongful actions, inaction, and omissions were fraudulent, misleading and illegal, and would directly and proximately cause Plaintiffs and Class Members to suffer the above-described damages. All of Plaintiffs' and Class Members' damages were reasonably foreseeable by Schnucks, and anticipated as a substantial factor and a natural consequence of its pattern of unlawful activity.

COUNT III

VIOLATION OF 18 U.S.C. § 1962(d) BY CONSPIRING TO VIOLATE 18 U.S.C. § 1962(c)
(On behalf of the Nationwide Class and State Sub-Classes)

104. The preceding factual statements and allegations are incorporated by reference.

105. Each Plaintiff and each Class Member is a "person" within the meaning of 18 U.S.C. §§ 1961(3), 1964(c). Each Plaintiff and each Class Member also is a "financial institution" within the meaning of 18 U.S.C. § 1344.

106. Schnucks is a "person" within the meaning of 18 U.S.C. §§ 1961(3) and 1962(a).

107. The Visa Network and MasterCard Network are "enterprises" within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c) and, at all relevant times, were engaged in, and the activities of which affected, interstate commerce within the meaning of 18 U.S.C. §§ 1961(4), 1962(c), 1962(d).

108. Schnucks conspired with other persons and entities, the identities of whom are

known only to Schnucks at this time and await discovery, within the meaning of 18 U.S.C. § 1962(d) to violate 18 U.S.C. § 1962(c); that is, Schnucks and its co-conspirators conspired to manage and operate the Visa and MasterCard Networks, and conduct and participate in the business and financial affairs of the Visa and MasterCard Networks (the enterprises), through a pattern of unlawful activity within the meaning of 18 U.S.C. §§ 1961(1)(B), 1961(5), and 1962(c)—to wit, the above-described open-ended, unlawful and fraudulent schemes to cheat and defraud Plaintiffs and Class Members to obtain money, funds, credits, assets, and other property owned by, or under the custody or control of, Plaintiffs and Class Members by means of false or fraudulent pretenses and intentional misrepresentations. Alternatively, Schnucks fraudulently and intentionally failed to disclose to Plaintiffs and Class Members that the reverse was true.

109. As a direct and proximate result of Schnucks' above-described multiple and repeated acts of interstate wire fraud and bank fraud, Plaintiffs and Class Members have suffered (and will continue to suffer) damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Schnucks also (i) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (ii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members.

110. Schnucks and its co-conspirators intentionally participated in a conspiracy to engage in the above-described interstate wire fraud, bank fraud, unlawful and intentional schemes, wrongful actions, inaction, and omissions for Schnucks' financial benefit and to

Plaintiffs' and Class Members' financial detriment in violation of 18 U.S.C. §§ 1343 and 1344. The members, time and place of this complex, multi-party conspiracy are known only by Schnucks at this time and await discovery.

111. As described above, Schnucks and its co-conspirators managed and operated the Visa and MasterCard Networks (the enterprises) in such a way as to engage in the above-described multiple predicate acts of interstate wire fraud and bank fraud for the purpose of increasing Schnucks' profitability and return on investment to Plaintiffs' and Class Members' financial detriment.

112. Schnucks knew, or recklessly should have known, its unlawful and intentional conspiracy and commission of the above-described interstate wire fraud, bank fraud, wrongful actions, inaction, and omissions were fraudulent, misleading and illegal, and would directly and proximately cause Plaintiffs and Class Members to suffer the above-described damages. All of Plaintiffs' and Class Members' damages were reasonably foreseeable by Schnucks, and anticipated as a substantial factor and a natural consequence of its pattern of unlawful activity.

COUNT IV

BREACH OF FIDUCIARY DUTY
(On behalf of the Nationwide Class and State Sub-Classes)

113. The preceding factual statements and allegations are incorporated by reference.

114. By providing Schnucks with the private, non-public, confidential, and sensitive payment card information and other customer data, Plaintiffs and Class Members placed their trust and confidence in the faithful integrity of Schnucks, which gained superiority and influence over Plaintiffs and Class Members with respect to such payment card information and customer data, to safeguard and protect it. While in the possession, custody, and control of Schnucks, Plaintiffs and Class Members had no access to, or control over, such data.

115. By receiving Plaintiffs' and Class Members' confidential and sensitive payment

card information and other customer data, Schnucks assumed responsibility of, and control over, it and, in fact, assumed the role of a trustee to safeguard and protect it. As such, Schnucks, Plaintiffs, and Class Members were (and continue to be) in confidential, special, and fiduciary relationships, pursuant to which Schnucks had (and continues to have) a duty to safeguard and protect such confidential and sensitive payment card information and other customer data. Plaintiffs and Class Members expected and, in fact, trusted Schnucks to exercise, at the very least, a reasonable degree of care to safeguard and protect the confidential and sensitive payment card information and other customer data; Schnucks was well aware of Plaintiffs' and Class Members' expectations and trust.

116. As a fiduciary, Schnucks owed (and continues to owe) Plaintiffs and Class Members (i) the commitment to deal fairly and honestly, (ii) the duties of good faith and undivided loyalty, and (iii) integrity of the strictest kind. Schnucks was (and continues to be) obligated to exercise the highest degree of care in carrying out its obligations to Plaintiffs and Class Members under the Parties' confidential, special, and fiduciary relationships including, without limitation, safeguarding and protecting Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data.

117. Schnucks breached its fiduciary duty to Plaintiffs and Class Members by failing to identify, implement, maintain, and monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security and confidentiality of Plaintiffs' and Class Members' private, non-public, confidential and sensitive payment card information and other customer data by, *inter alia*:

a. failing to delete payment card information after the time period necessary to authorize the 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 ("PII") (such as, without limitation, confidential and sensitive payment card information and other customer data) 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 PII from its network while the Data Breach was taking place.

Schnucks also breached its fiduciary duty to Plaintiffs and Class Members by failing to (i) advise Plaintiffs and Class Members that the appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems within its computer systems and servers, in fact, were not in place, properly functioning and monitored (but misrepresenting the exact opposite was true), and (ii) timely notify them of the Data Breach so they could take the necessary defensive steps to minimize their damages and other actual injury and harm. In doing so, Schnucks acted intentionally, wantonly, recklessly, and with a complete disregard for Plaintiffs' and Class Members' rights and interests, and the consequences of its actions.

118. As a direct and proximate result of Schnucks' above-described breach of the

fiduciary duty it owed (and continues to owe) Plaintiffs and Class Members, they have suffered (and will continue to suffer) damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage. Schnucks' wrongful conduct constitutes breach of fiduciary duty at common law.

COUNT V

NEGLIGENCE/GROSS NEGLIGENCE
(On behalf of the Nationwide Class and State Sub-Classes)

119. The preceding factual statements and allegations are incorporated by reference.

120. By receiving Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data, and entering into the above-described confidential, special, and fiduciary relationships, Schnucks owed (and continues to owe) them the duty to exercise reasonable care in safeguarding and protecting the confidential and sensitive payment card information and other customer data from being unlawfully disclosed and compromised.

121. 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, Class Members, and their customers could take the appropriate steps necessary to minimize their damages. 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 to their businesses and property, (ii) saved the cost of implementing the proper customer data 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. Schnucks' duty to properly and timely disclose the Data Breach to Plaintiffs, Class Members, and their customers also arises from the above-described sources.

122. Schnucks also had a duty to implement the appropriate data security policies, procedures, protocols, and hardware and software systems across its computer systems to prevent and detect data breaches and the unauthorized dissemination of Plaintiffs' and Class Members' customers' private, non-public, confidential and sensitive financial information—including the payment card information and other customer data wrongfully disclosed and compromised by the Schnucks Data Breach. Such duty also arises from the same above-described sources. By and through its above-described intentional false representations to the contrary, intentional false omissions, and intentional silence when it had a duty to speak, on which Plaintiffs and Class Members relied, and wrongful actions and inaction, Schnucks unlawfully breached its duties to Plaintiffs and Class Members by, *inter alia*, (i) failing to implement the appropriate customer 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) intentionally lulling Plaintiffs and Class Members into a false sense of security that such customer data security policies, procedures, protocols, and hardware and software systems were in place and functioning across its computer network. Had Plaintiffs and Class Members known such representations and omissions were false, they would have embarked on a different course

of action, and taken the appropriate steps to safeguard and protect the compromised confidential and sensitive payment card information and other customer data themselves.

123. Schnucks' above-referenced duties arose from the common law, in part, because it was reasonably foreseeable to Schnucks under the circumstances that a data breach of its internal computer systems was likely to occur that would cause Plaintiffs' and Class Members' above-described damages. Schnucks' duties also arose from the duties expressly imposed upon Schnucks by other sources, such as industry standards (*i.e.*, PCI DSS), best practices, implied contracts between Schnucks and Plaintiffs and Class Members, contracts between Schnucks and other third parties (such as Citicorp and First Data), and participation in the Visa and MasterCard Networks (and the corresponding Visa Operating Regulations and MasterCard Rules).

124. Schnucks' duties also arose from Section 5 of the FTC Act, which 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 PII, such as Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data.

125. Schnucks intentionally or negligently breached its common law, statutory, and other duties by 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 compromised by the Data Breach, and by failing to provide timely notice of the Breach. Schnucks' specific negligent acts and omissions include, *inter alia*:

a. failing to delete payment card information after the time period necessary to authorize the 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 PII at the point-of sale;

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

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

l. 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 PII from its network while the Data Breach was taking place.

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

126. As a direct and proximate result of Schnucks' above-described intentional false representations, intentional false omissions, and intentional silence when it had a duty to speak, on which Plaintiffs and Class Members relied, wrongful actions, and inaction, Plaintiffs and Class Members have suffered (and will continue to suffer) damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

127. The economic loss doctrine does not bar Plaintiffs' and Class Members' negligence and gross negligence claims because (i) their above-described damages, injury and harm were directly and proximately caused by Schnucks' above-described intentional false representations, intentional false omissions, and intentional silence when it had a duty to speak (on which Plaintiffs and Class Members justifiably relied), or, in the alternative, Schnucks' negligent and grossly negligent misrepresentations and omissions (on which Plaintiffs and Class Members justifiably relied), (ii) Plaintiffs, Class Members, and Schnucks were (and continue to be) in confidential, special, and fiduciary relationships that Schnucks breached (as described above), (iii) 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 electronic transactions), (iv) Schnucks breached various public duties including, *inter alia*, its common law and statutory duty 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 Breach, and observe and comply with Section 5 of the FTC Act, 15 U.S.C. § 45, and (v) Schnucks engaged in the above-described intentional, negligent, and grossly negligent conduct.

COUNT VI

NEGLIGENCE *PER SE*
(On behalf of the Nationwide Class and State Sub-Classes)

128. The preceding factual statements and allegations are incorporated by reference.

129. 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 PII, such as Plaintiffs' and Class Members' confidential and sensitive payment card information and other customer data.

130. Schnucks violated Section 5 of the FTC Act (and similar state statutes) by 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' conduct was particularly unreasonable given the nature and amount of PII 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 Plaintiffs and Class Members.

131. Plaintiffs and Class Members are within the class of persons Section 5 of the FTC Act and similar state statutes are designed to protect as they are engaged in trade and commerce, and bear primary responsibility for reimbursing consumers for fraud losses. In fact, many Plaintiffs and Class Members are credit unions organized as cooperatives whose members are consumers.

132. Moreover, the injury and harm suffered by Plaintiffs and Class Members is the type of injury and harm the FTC Act (and similar state statutes) 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.

133. By its above-described wrongful actions, inaction, and omissions, Schnucks also failed to comply with industry best practices, the PCI DSS, Visa Operating Regulations, and MasterCard Rules. Plaintiffs and Class Members are members of the class of persons intended to

be protected by the PCI DSS, Visa Operating Regulations, MasterCard Rules, and other industry data security standards and best practices. The injury and harm suffered by Plaintiffs and Class Members is the type of injury and harm industry best practices, the PCI DSS, Visa Operating Regulations, and MasterCard Rules are intended to guard against. Schnucks' violation of the Visa Operating Regulations and MasterCard Rules, the details of which await discovery, will most likely result in fines and other sanctions imposed by Visa and MasterCard.

134. Schnucks' violations of Section 5 of the FTC Act (and similar state statutes), industry best practices, the PCI DSS, Visa Operating Regulations, and MasterCard Rules constitute negligence *per se* at common law.

135. 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 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

COUNT VII

NEGLIGENT MISREPRESENTATION
(On behalf of the Nationwide Class and State Sub-Classes)

136. The preceding factual statements and allegations are incorporated by reference.

137. By receiving Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data, and entering into the above-described confidential, special, and fiduciary relationships, Schnucks owed (and continues to owe) them the duty to exercise reasonable care in safeguarding and protecting the payment card

information and other customer data from being unlawfully disclosed and compromised, as well as the duty to communicate accurate information should Schnucks not properly safeguard and protect the payment card information and other customer data (*e.g.*, putting Plaintiffs and Class Members on notice, so they could take the appropriate steps to alert their customers, and safeguard and protect the compromised payment card information themselves).

138. Schnucks also had an after-the-fact 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, Class Members, and their customers could take the appropriate steps necessary to minimize their damages. 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) saved the cost of implementing the proper customer data security policies, procedures, protocols, and hardware and software systems, and (ii) wrongfully shifted the risk and expense of the Data Breach to Plaintiffs and Class Members. Schnucks' duty to properly and timely communicate accurate information about the Data Breach on a timely basis to Plaintiffs, Class Members, and their customers arises from the above-described sources.

139. Schnucks knew Plaintiffs and Class Members are part of the Visa and MasterCard Networks, and rely on merchants that accept Visa and MasterCard payment cards to implement the appropriate customer data security policies, procedures, protocols, and hardware and software systems across their internal computer networks.

140. By its above-described wrongful actions, inaction, and omissions, Schnuck carelessly and negligently made numerous misrepresentations to Plaintiffs and Class Members in the form of material omissions (*i.e.*, the failure to disclose) that (i) it was not in compliance with

the Visa Operating Regulations and MasterCard Rules, (ii) it was not in violation of Section 5 of the FTC Act mandating the protection of payment card information, (iii) it was not in compliance with the PCI DSS, (iv) it was not in compliance with industry standards and best practices, and (v) its customer data security policies, procedures, protocols, and hardware and software systems would not safeguard and protect sensitive customer data—including the payment card information and other customer data compromised in the Data Breach. Schnucks also failed to properly and 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.

141. Schnucks intentionally made such misrepresentations in the form of material omissions during the course of Schnucks' business (i) for the guidance of a limited group of persons in connection with a particular business transaction; to wit, Plaintiffs and Class Members in connection with Schnuck's electronic payment card transactions utilizing payment cards issued by Plaintiffs and Class Members, and (ii) to induce Plaintiffs and Class Members to issue payment cards used to make purchases at Schnucks and approve millions of electronic payment card transactions made at Schnucks via the interstate wires. Because of Schnucks' above-described failure to exercise reasonable care, such omissions were false when made.

142. Plaintiffs and Class Members justifiably relied on Schnucks' misrepresentations in the form of material omissions, and issued payment cards used to make purchases at Schnucks and approve millions of electronic payment card transactions at Schnucks via the interstate wires. As a direct and proximate result of their reliance on Schnucks' above-described careless and negligent misrepresentations in the form of material omissions, Plaintiffs and Class Members have suffered (and will continue to suffer) damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

143. Had Plaintiffs and Class Members known such representations and omissions were false, they would have embarked on a different course of action, and taken the appropriate steps to safeguard and protect the compromised confidential and sensitive payment card information and other customer data themselves. Schnucks' above-described wrongful actions, inaction, and material omissions constitute negligent misrepresentations at common law.

COUNT VIII

BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class and State Sub-Classes)

144. The preceding factual statements and allegations are incorporated by reference.

145. Schnucks required the private, non-public, confidential, and sensitive payment card information and other customer data compromised by the Data Breach in order to facilitate electronic payment card transactions. Implicit in this requirement was a covenant requiring Schnucks to, *inter alia*, take reasonable efforts to safeguard and protect the confidential and sensitive payment card information and other customer data, and promptly notify Plaintiffs, Class Members, and their customers in the event their payment card information and other customer data was wrongfully disclosed and compromised.

146. By repeatedly and systematically requesting the authorization of millions of

electronic payment card transactions via the interstate wires, Schnucks impliedly promised Plaintiffs and Class Members that its customer data security policies, procedures, protocols, and hardware and software systems across its internal computer network properly safeguarded and protected Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data from unauthorized dissemination.

147. Plaintiffs and Class Members lived up to their obligations by reviewing and authorizing millions of electronic payment card transactions via the interstate wires. Notwithstanding its above-described obligations, however, Schnucks knowingly or recklessly failed to safeguard and protect Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data by providing a gateway to fraudsters who targeted Schnucks' unprotected computer systems and unprotected payment card information, spent months harvesting the information, and used, sold, and transferred the information to other fraudsters and unauthorized third parties worldwide without authorization.

148. 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 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

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

COUNT IX

BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS ARE THIRD-PARTY BENEFICIARIES
(On behalf of the Nationwide Class and State Sub-Classes)

150. The preceding factual statements and allegations are incorporated by reference.

151. At all relevant times, Schnucks was (and continues to be) in contractual relationships with (i) Citicorp, its acquiring bank for payment card transactions, (ii) First Data, its payment card transaction processor, and (iii) Schnucks' outside computer systems consultants and vendors. Plaintiffs and Class Members are intended third-party beneficiaries of these contracts.

152. Such contracts explicitly or implicitly require Schnucks to implement customer data security policies, procedures, protocols, and hardware and software systems across its computer systems to safeguard and protect Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data from unauthorized release, disclosure, and dissemination.

153. Plaintiffs and Class Members are intended third-party beneficiaries of these contracts. 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.

154. By its above-described wrongful actions, inaction, and omissions, and the resulting Data Breach, Schnucks breached one or more of these contracts by, *inter alia*, failing to safeguard and protect Plaintiffs' and Class Members' private, non-public, confidential, and sensitive payment card information and other customer data wrongfully disclosed and compromised in the Data Breach, which directly and proximately caused Plaintiffs and Class Members to suffer damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

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

COUNT X

VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT

(On behalf of the Illinois State Sub-Class)

156. The preceding factual statements and allegations are incorporated by reference.

157. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/1, *et seq.* (the "Act"), prohibits unfair methods of competition and unfair acts or practices. In determining whether an act or practice is unfair, the Act expressly requires consideration of interpretations of Section 5 of the FTC Act. *See* 815 Ill. Comp. Stat. 505/2.

158. Schnucks engaged in unfair and unlawful business practices, in violation of the Act, by failing to implement and maintain reasonable data security measures, violating industry standards, such as the PCI DSS, and committing the other above-described wrongful actions and omissions that caused the Data Breach.

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

160. Schnucks' above-described wrongful actions, inaction, and omissions directly and proximately caused substantial injury and harm to Plaintiffs CTB, 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.

161. Plaintiffs CTB, 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.

162. Schnucks' practice of maintaining inadequate data security measures provided no benefit to Plaintiffs, Class Members, consumers, and competition in general. The substantial injury and harm sustained by Plaintiffs CTB, 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 responsible for safeguarding and protecting confidential and sensitive payment card information and other customer data, Plaintiffs CTB, UIECU, FFSB, the Illinois Sub-Class Members, and Class Members operating in Illinois could not have known about Schnucks' inadequate data security practices, and could not have avoided their damages, injuries, and harm.

163. As a direct and proximate result of Schnucks' above-described unfair and unlawful business practices, Plaintiffs CTB, 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 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage—for which they are entitled to compensation. Plaintiffs CTB, UIECU, FFSB, the Illinois Sub-Class Members, and Class Members operating in Illinois also are entitled to recover their attorneys' fees, litigation expenses, and costs, and injunctive and declaratory relief.

COUNT XI

UNJUST ENRICHMENT/ASSUMPSIT
(On behalf of the Nationwide Class and State Sub-Classes)

164. The preceding factual statements and allegations are incorporated by reference.

165. Plaintiffs plead this Count in the alternative to its contract claims (Counts VIII and IX) because they cannot recover under this Count and under Counts VIII and IX.

166. Plaintiffs and Class Members conferred a benefit on Schnucks in the form of approved electronic payment card transactions utilizing the wrongfully disclosed and compromised payment cards they issued over the interstate wires, which allowed Schnucks to consummate food and merchandise sales to its customers that, in turn, generated revenue and profits for Schnucks. Schnucks (and possibly others, the identities of whom are known only to Schnucks at this time), therefore, have been (and continue to be) unjustly enriched by, *inter alia*, (i) the revenue and profits from electronic payment card transactions approved by Plaintiffs and

Class Members over the interstate wires that were made on the wrongfully disclosed and compromised payment cards, from December 2012 through March 30, 2013, the date Schnucks first reported the Data Breach to the general public, (ii) the shifted risk and expense of the Data Breach to Plaintiffs and Class Members, (iii) using and investing the fraudulently obtained revenue and profits from the payment card transactions described in (i) to participate in, create, and operate various enterprises including, *inter alia*, the Visa Network and the MasterCard Network, and (iv) the return on investment on the amounts described in (i)-(iii) (above).

167. 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 doctrines of unjust enrichment and the duty to make restitution under the common law equitable doctrine of assumpsit.

COUNT XII

EQUITABLE SUBROGATION
(On behalf of the Nationwide Class and State Sub-Classes)

168. The preceding factual statements and allegations are incorporated by reference.

169. Subrogation compels the ultimate payment of a debt by one who is primarily responsible for the loss and, in justice, equity and good conscience, should pay it. Equitable subrogation has as its aim the advancement of justice, and the prevention of injustice.

170. As a direct and proximate result of Schnucks' above-described wrongful actions, inaction, and omissions, it is indisputable that Schnucks is *entirely* responsible for the Data Breach and Plaintiffs' and Class Members' damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii)

increased fraud monitoring on potentially impacted accounts, and (iv) lost interest and transaction fees due to reduced payment card usage.

171. As the party entirely responsible for the Data Breach, and Plaintiffs' and Class Members' resulting damages, injuries, and harm, Schnucks, in justice, equity and good conscience, should be compelled to reimburse Plaintiffs' and Class Members' damages, injuries, and harm under the common law doctrine of equitable subrogation.

COUNT XIII

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

172. The preceding factual statements and allegations are incorporated by reference.

173. 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 federal and state statutes.

174. An actual controversy exists in the wake of the Data Breach regarding Schnucks' common law and statutory duties to reasonably safeguard and protect Plaintiffs' and Class Members' confidential and sensitive payment card information and other customer data. Schnucks' data security measures were (and continue to be) woefully inadequate. Plaintiffs and Class Members continue to suffer damages to their businesses and property, and other injury and harm, as additional fraudulent charges are made on compromised payment cards issued to Schnucks' customers.

175. **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, Visa Operating Regulations, MasterCard 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, and absorbed fraudulent charges made on payment cards compromised by the Breach, are legally entitled to recover compensation for their damages, injury, and harm from Schnucks.

176. **INJUNCTIVE RELIEF.** The above-described repetitious and systematic interstate wire fraud and bank fraud, in violation of 18 U.S.C. §§ 1343 and 1344, engaged in by Schnucks (and its co-conspirators) 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) 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, Visa Operating Regulations, MasterCard Rules, 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 (and its co-conspirators) have been unjustly enriched, and (iii) discontinue its above-described unlawful, intentional, fraudulent, and cheating schemes, wrongful actions, inaction, and omissions. Plaintiffs and Class Members also are entitled to injunctive relief requiring Schnucks to implement and maintain 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. All conditions precedent to Plaintiffs' and Class Members' claims for relief have been performed and occurred. 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.

177. 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.

178. 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 customer data security measures, the cost to Schnucks of complying with an injunction requiring the institution of customer data security measures they are already required to implement is relatively minimal.

179. 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 injury and harm that would be suffered by Plaintiffs, Class Members, and the millions of consumers confidential and sensitive payment card information and other customer data would be compromised.

RELIEF REQUESTED

180. The preceding factual statements and allegations are incorporated by reference.

181. **ACTUAL, CONSEQUENTIAL, AND INCIDENTAL DAMAGES.** As a direct and proximate result of the above-described unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions engaged in by Schnucks (and its co-conspirators), Plaintiffs and Class Members have sustained (and will continue to sustain) actual, consequential, incidental, and statutory damages to their businesses and property, and other 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) absorption and refund of fraudulent charges made on the compromised payment cards, (iii) increased fraud monitoring on potentially impacted accounts, and (iv) 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 (and its co-conspirators) 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.

182. **PUNITIVE DAMAGES.** The above-described unlawful and intentional schemes, wrongful actions, inaction, and omissions engaged in by Schnucks (and its co-conspirators) were committed intentionally, 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 (and its co-conspirators) 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.

183. **TREBLE DAMAGES.** Plaintiffs and Class Members also are entitled to automatic treble damages for the above-described unlawful and intentional schemes to cheat and defraud, wrongful actions, inaction, and omissions engaged in by Schnucks (and its co-conspirators) under 18 U.S.C. § 1964(c).

184. **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*, 18 U.S.C. § 1964(c), 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:

(a) With respect to Counts I–III (violations of 18 U.S.C. § 1961, *et seq.*)--

(i) threefold the actual, consequential, and incidental damages sustained by Plaintiffs and Class Members, along with attorneys' fees, litigation expenses, and court costs, all pursuant to 18 U.S.C. § 1964(c), together with pre- and post-judgment interest at the highest legal rates;

(ii) equitable relief, as may be appropriate, pursuant to 18 U.S.C. § 1964(a) or other law, including an equitable accounting for all benefits, consideration, revenues, profits, and earnings received, directly or indirectly, by Schnucks (and its co-conspirators) 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 (and its co-conspirators) have been unjustly enriched; and

(iii) injunctive and declaratory relief (as set forth above).

(b) With respect to Counts IV–XIII:

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

(ii) punitive damages;

(iii) all amounts by which Schnucks (and its co-conspirators) have been unjustly enriched;

(iv) an equitable accounting for all benefits, consideration, revenues, profits, and earnings received, directly or indirectly, by Schnucks (and its co-conspirators) 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 (and its co-conspirators) have been unjustly enriched;

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

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

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

(c) For all Counts, 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 9, 2015.

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