IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

SELCO COMMUNITY CREDIT UNION, Individually and on Behalf of a Class of Similarly Situated Financial Institutions, Plaintiff, v. NOODLES & COMPANY, Defendant.	Case No: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff SELCO Community Credit Union ("Plaintiff"), through its undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, files this Class Action Complaint against Defendant Noodles & Company ("Noodles" or "Defendant") and states the following:

INTRODUCTION

1. This is a class action on behalf of credit unions, banks, and other financial institutions that suffered injury as a result of a security breach beginning on or around late January 2016, to the present, that compromised the names, credit and debit card numbers, card expiration dates, card verification values ("CVVs"), and other credit and debit card information (collectively, "Payment Card Data") of customers of 322 nationwide locations of Defendant's Noodles & Company brand restaurants (hereinafter, the "Noodles Data Breach").

2. The Noodles Data Breach forced Plaintiff and other financial institutions to: (a) cancel or reissue any credit and debit cards affected by the Noodles Data Breach; (b) close any

deposit, transaction, checking, or other accounts affected by the Noodles Data Breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) open or reopen any deposit, transaction, checking, or other accounts affected by the Noodles Data Breach; (d) refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Noodles Data Breach; (e) respond to a higher volume of cardholder complaints, confusion, and concern; (f) increase fraud monitoring efforts; and (g) reissue compromised cards.

3. In addition, the Noodles Data Breach caused Plaintiff and the members of the Class to lose revenue, as a result of a decrease in card usage, after the breach was disclosed to the public.

4. As alleged herein, the injuries to Plaintiff and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for customer information, including credit and debit card data and personally identifying information. Defendant failed to take steps to employ adequate security measures despite well-publicized data breaches at large, national retail and restaurant chains in recent months, including Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Wendy's, Dairy Queen, and Kmart.

5. The failure of Defendant to adequately secure its data networks was particularly inexcusable given the fact that the infiltration underlying the Noodles Data Breach involved mostly the same techniques as those used in major data breaches in the preceding months and years, including the well-publicized data breaches at restaurant chains like P.F. Chang's, Wendy's, and Dairy Queen. Nevertheless, despite having knowledge that such data breaches

were occurring throughout the restaurant industry, Defendant failed to properly protect sensitive payment card information.

6. The data breach was the inevitable result of Noodles' inadequate data security measures and approach to data security. Despite the well-publicized and ever-growing threat of cyber breaches involving payment card networks and systems, Noodles systematically failed to ensure that it maintained adequate data security measures, failed to implement best practices, failed to upgrade security systems, and failed to comply with industry standards by allowing its computer and point of sale systems to be hacked causing financial institutions' payment card and customer information to be stolen. Noodles' data security deficiencies were so significant that hackers were able to install malware and remain undetected for months, until outside parties notified Noodles that its computer and point of sale systems may have been breached as a result of the identification of fraudulent transactions that had taken place after the hackers had used or sold the Customer Data.

7. Defendant also failed to mitigate the damage of a potential data breach by failing to implement chip-based card technology, otherwise known as EMV technology. EMV – which stands for Europay, MasterCard, and Visa – is a global standard for cards equipped with computer chips and technology used to authenticate chip card transactions. While Visa implemented minimum EMV Chip Card and Terminal Requirements in October 2015, Defendant has not implemented EMV technology in its stores, and thus, left all of the information on the magnetic stripe of cards used in its restaurant locations vulnerable to theft in a way it has been repeatedly warned about.

8. In addition to failing to prevent the intrusion in the first instance, and failing to implement required data security measures that would have limited its ability to affect cardholders and the financial institutions from which their cards came, Defendant exacerbated injury by failing to notify customers of the infiltration for a period of at least six weeks from the first media reports that the Noodles Data breach had occurred, after letting the breach itself go undetected for almost four months. According to the security experts Defendant is working with, the Noodles store payment data systems were infected with a form of malware of which Defendant was unaware until mid-May 2016. Therefore, the volume of data stolen was much greater than it would have been had Defendant maintained sufficient malware monitoring to identify and eliminate the breach as it was occurring.

9. As a direct and proximate consequence of Defendant's negligence, vast amounts of customer information were stolen from the Noodles computer network. Though an investigation is still ongoing, it appears that hundreds of thousands of Defendant's customers at 322 locations nationwide have had their credit and debit numbers compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Moreover, Plaintiff and members of the Class have incurred and will continue to incur significant costs associated with, among other things, notifying their customers of issues related to the Noodles Data Breach, closing out and opening new customer accounts, reissuing customers' cards, and/or refunding customers' losses resulting from the unauthorized use of their accounts.

10. Plaintiff and the members of the Class seek to recover damages caused by Defendant's negligence, negligence *per se*, and for declaratory and injunctive relief.

PARTIES

11. Plaintiff SELCO Community Credit Union is a credit union headquartered at 299 East 11th Avenue, Eugene, Oregon 97401. As a result of the Noodles Data Breach, Plaintiff has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

12. Defendant Noodles & Company ("Noodles") is a Delaware corporation with a principal executive office located at 520 Zang Street, Suite D, Broomfield, Colorado 80021. Noodles operates a chain of fast-casual restaurants "where its globally inspired dishes come together to create a World Kitchen." Noodles operates approximately 492 restaurants in 35 states, the District of Columbia, and one Canadian province. Of those stores, 422 are owned by Noodles and 70 are franchised. In 2015, its revenues totaled approximately $450 million dollars.

JURISDICTION AND VENUE

13. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. §1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class, defined below, many of which are citizens of a different state than Defendant. Defendant Noodles is a citizen of Delaware, where it is incorporated, and Colorado, where its principal place of business is located.

14. The District of Colorado has personal jurisdiction over Defendant because Defendant is found within this District and conducts substantial business in this District.

15. Venue is proper in this Court pursuant to 28 U.S.C. §1391, because Defendant resides in this judicial district, regularly transacts business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

FACTUAL BACKGROUND

A. Background on Electronic Debit and Credit Card Transactions and Requirements for Securing Data

16. Plaintiff and the members of the Class are financial institutions that issue payment cards[1] to their customers.

17. Noodles stores accept customer payment cards for the purchase of goods and services. At the point of sale ("POS"), these cards are swiped on a POS terminal, and either a personal identification number (or some other confirmation number) is entered, or a receipt is signed to finish the transaction on behalf of the customer.

18. It is well known that customer Payment Card Data is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and restaurants nationwide, including The Home Depot, Target, Kmart, Wendy's, P.F. Chang's, Neiman Marcus, and many others. Noodles was aware of the prevalence of data breaches among retailers and acknowledged the risk of a data breach of its own, as stated in its most recent Form 10-K filed with the Securities Exchange Commission:

> Other restaurants and retailers have experienced security breaches in which credit and debit card information has been stolen. We may in the future become subject to claims for purportedly fraudulent transactions arising out of the actual or

[1] These cards include, for example, debit or credit cards branded with the VISA or MasterCard logo.

> alleged theft of credit or debit card information, and we may also be subject to lawsuits or other proceedings relating to these types of incidents.[2]

Despite widespread publicity and industry alerts regarding these other notable data breaches, Noodles failed to take reasonable steps to adequately protect its computer systems from being breached.

19. A large portion of sales at Noodles' restaurants are made to customers using credit or debit cards. A basic description of the various steps necessary to execute a credit/debit card transaction is as follows: (1) after the credit/debit card is swiped, the merchant (*e.g.*, Noodles) uses one of several payment processing networks (*e.g.*, Visa or MasterCard) to transmit a request for authorization to the institution that issued the payment card (*e.g.*, Plaintiff); (2) the issuing institution authorizes the payment and the merchant electronically forwards a receipt of the transaction to another financial institution known as the "acquiring bank," which contracts with the merchant to process credit and debit card transactions on the merchant's behalf; (3) the acquiring bank forwards the funds to the merchant to satisfy the transaction, and is then reimbursed by the issuing financial institution (*e.g.*, Plaintiff); and (4) finally, the issuing institution posts the debit or credit transaction to its customer's account.

20. Noodles is, and at all relevant times has been, aware that the Payment Card Data it maintains is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

---

[2] Noodles & Co., Annual Report (Form 10-K) (Mar. 1, 2016), available at https://www.sec.gov/Archives/edgar/data/1275158/000127515816000096/a10k2015.htm (last visited Sept. 6, 2016).

21. Noodles is, and at all relevant times has been, aware of the importance of safeguarding its customers' Payment Card Data and of the foreseeable consequences that would occur if its data security systems were breached, specifically including the significant costs that would be imposed on issuers, such as the Plaintiff and members of the Class, and others. In its notice relating to the Noodles Data Breach, Noodles notes that "[g]uests should immediately report any unauthorized charges to their card issuer."[3]

22. Given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, it is unsurprising that financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure consumers' valuable data is protected.

23. The Payment Card Industry Data Security Standards ("PCI DSS") is a list of 12 information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted and requires merchants like Defendant to 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.

24. The 12 requirements of the PCI DSS are:

[3] Press Release, Noodles & Company, Noodles & Company Provides Notice of Data Security Incident (June 28, 2016), http://www.noodles.com/security/ (last visited Sept. 6, 2016).

Build and Maintain a Secure Network

(1) Install and maintain a firewall configuration to protect cardholder data

(2) Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

(3) Protect stored cardholder data

(4) Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

(5) Protect all systems against malware and regularly update anti-virus software or programs

(6) Develop and maintain secure systems and applications

Implement Strong Access Control Measures

(7) Restrict access to cardholder data by business need to know

(8) Identify and authenticate access to system components

(9) Restrict physical access to cardholder data

Regularly Monitor and Test Networks

(10) Track and monitor all access to network resources and cardholder data

(11) Regularly test security systems and processes

Maintain an Information Security Policy

(12) Maintain a policy that addresses information security for all personnel.[4]

[4] PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2*, at 9 (May 2016), https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1472840893444 (last visited Sept. 6, 2016).

25. Furthermore, PCI DSS 3.1 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates. Defendant was at all times fully aware of its data protection obligations for Noodles stores in light of their participation in the payment card processing networks and their daily collection and transmission of tens of thousands of sets of payment card data.

26. Furthermore, Defendant knew that because they accepted payment cards at Noodles stores containing sensitive financial information, customers and financial institutions, such as Plaintiff, were entitled to, and did, rely on Defendant to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

27. In addition, the payment card industry also set rules requiring all businesses to upgrade to new card readers that accept EMV chips. EMV chip technology uses embedded computer chips instead of magnetic stripes to store Payment Card Data. Unlike magnetic stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the thieves, making it much more difficult for criminals to profit from what is stolen.

28. The payment card industry (MasterCard, Visa, Discover, and American Express) set a deadline of October 1, 2015, for businesses to transition their systems from magnetic stripe to EMV technology. Noodles did not meet that deadline.

29. Under Card Operating Regulations, businesses accepting payment cards, but not meeting the October 1, 2015 deadline, agree to be liable for damages resulting from any data breaches.

30. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by §5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. §45.

31. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

32. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[5]

[5] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Nov. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-

33. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses in regard to their data security obligations.

B. The Noodles Data Breach: the Result of Lax Security Standards

34. On May 16, 2016, *Krebs on Security* reported that multiple sources at multiple financial institutions had "detected a pattern of fraudulent charges on customer cards that were used at various Noodles & Company locations between January 2016 and the present."[6] When asked to comment, Noodles stated that it was "currently investigating some unusual activity reported to us Tuesday, May 16, 2016 by our credit card processor. Once we received this report, we alerted law enforcement officials and we are working with third party forensic experts. Our investigation is ongoing and we will continue to share information." *Id.* But that investigation did not begin until its credit card processor reported unusual activity. Noodles did not report it began a third-party investigation until May 20, 2016, after it had been ousted by Krebs. *Id*.

35. While Krebs noted that the "investigation comes amid a fairly constant drip of card breaches at main street retailers, restaurant chains and hospitality firms," and that "U.S. banks have been transitioning to providing customers more secure chip-based credit and debit cards[.] . . . The chip encrypts the card data and makes it much more difficult and expensive for thieves to counterfeit cards," Noodles has not yet implemented a chip card system. *Id*. As

---

personal-information-guide-business_0.pdf (last visited Sept. 6, 2016).

[6] *See* Krebs on Security, *Noodles & Company Probes Breach Claims* (May 19, 2016), http://krebsonsecurity.com/2016/05/noodles-company-probes-breach-claims/ (last accessed Sept. 2, 2016).

Noodles said in May, "The ongoing program we have in place to aggressively test and implement chip-based systems across our network is moving forward[.] . . . We are actively working with our key business partners to deploy this system as soon as they are ready." *Id*.

36. On June 10, 2016, VISA and MasterCard released alerts letting financial institutions know that cards had been compromised as a result of the Noodles Breach, stating that the alerts are associated with the Noodles & Company investigation reported on by various popular blogging sites and news sources. However, this breach has yet to be confirmed by Noodles & Company.

37. Despite notice from financial institutions in May, and confirmatory investigations in early June, Noodles did not officially confirm the Noodles Data Breach until it released a statement on June 28, 2016, nearly six weeks later, saying that the breach "affected customers who used debit or credit cards at some of its locations between Jan. 31 and June 2." *Supra*, n.3.

38. In its notice, Noodles confirmed that "a recent data security incident may have compromised the security of payment information of some guests who used debit or credit cards at certain Noodles & Company locations between January 31, 2016 and June 2, 2016." *Id*.

39. Despite this notice, and while Noodles claims that customers may now use credit and debit cards at their stores without issue, Noodles conceded in its June 28, 2016 FAQ that it had not yet removed the malware at issue: "The Company is also working to implement additional procedures to further secure guests' debit and credit card information, including removing the malware at issue to contain this incident and to prevent any further unauthorized access to guests' debit or credit card information." *Id*.

40. Hackers infiltrated Noodles' payment data systems with malware that its systems could not detect, because its POS systems were inadequate. As security and consumer protection expert Brad Bussie points out, "[r]egarding the Noodles & Company breach . . . it's important to keep in mind that any malware needs a delivery mechanism."[7] He argues: "Payment card systems and point of sale systems should be completely isolated and hardened to create a minimal attack surface[.] . . . Organizations that allow removable devices, Internet browsing, and email on payment card networks are literally asking for a breach." *Id*. Noodles failed to secure its systems and the POS registers at its stores were infected with software that stole customer credit and debit card information from the registers. Based on the investigation, Noodles believes that credit and debit card numbers were compromised in the breach, but has still not yet informed its customers or Plaintiff of the scope of the breach.

41. The deficiencies in Noodles' security system include a lack of elementary security measures that even the most inexperienced IT professional could identify as problematic.

42. Had Noodles remedied the deficiencies in its IT systems, it could have prevented the Noodles Data Breach because virtually all data breaches are preventable. In fact, the *Online Trust Alliance*, a non-profit organization whose mission is to enhance online trust, user empowerment, and innovation, in its 2014 annual report, estimated that 740 million records were stolen in 2013, and that 89% of data breaches occurring in that year were avoidable.

---

[7] *See* eSecurity Planet, Jeff Goldman, *Omni Hotels, Noodles & Company, NC State Acknowledge Data Breaches* (July 12, 2016), http://www.esecurityplanet.com/network-security/omni-hotels-noodles-company-nc-state-acknowledge-data-breaches.html (last visited Sept. 2, 2016).

43. The security flaws outlined above, along with many others, were explicitly highlighted by VISA as early as 2009, when it issued a Data Security Alert describing the threat of RAM scraper malware.[8] The report instructs companies to "secure remote access connectivity," "implement secure network configuration, including egress and ingress filtering to only allow the ports/services necessary to conduct business" (*i.e.*, segregate networks), "actively monitor logs of network components, including intrusion detection systems and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "encrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit" and "work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration." *Id*.

44. In addition to ignoring explicit warnings from VISA, Noodles' security flaws also run afoul of industry best practices and standards. More specifically, the security practices in place at Noodles are in stark contrast and directly conflict with the Payment Card Industry Data Security Standards and requirements three and five of the 12 PCI DSS core security standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

45. As a result of industry warnings, industry practice, the PCI DSS, and multiple well-documented data breaches Defendant was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

---

[8] *Visa Security Alert* (Nov. 6, 2009), http://go.mercurypay.com/go/visa/targeted-hospitality-sector-vulnerabilities-110609.pdf (last visited Sept. 6, 2016).

46. Defendant was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used to access POS terminals since at least 2011, and specific types of malware, including RAM scraper malware, have been used recently to infiltrate large retailers such as Target, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Defendant was aware that malware is a real threat and is a primary tool of infiltration used by hackers.

47. Defendant received additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of POS malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware, which was updated on August 27, 2014.[9]

48. Despite the fact that Defendant was put on notice of the very real possibility of consumer data theft associated with its security practices and despite the fact that Defendant knew or, at the very least, should have known about the elementary infirmities associated with the Noodles security systems, it still failed to make necessary changes to its security practices and protocols.

49. Defendant knew that failing to protect customer card data would cause harm to the card-issuing institutions, such as Plaintiff and the Class, because the issuers are financially responsible for fraudulent card activity and must incur significant costs to prevent additional fraud.

---

[9] *See* United States computer Emergency Readiness Team, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (Aug. 27, 2014), https://www.us-cert.gov/ncas/alerts/TA14-212A (last visited Sept. 2, 2016).

50. Indeed, Defendant's public statements to customers after the data breach plainly indicate that Defendant believes that card-issuing institutions should be responsible for fraudulent charges on cardholder accounts resulting from the data breach. Noodles has made no overtures to the card-issuing institutions that are left to pay for damages as a result of the breach.

51. Defendant, at all times relevant to this action, had a duty to Plaintiff and members of the Class to: (a) properly secure payment card magnetic stripe information at the point of sale and on Defendant's internal networks; (b) encrypt payment card data using industry standard methods; (c) use and deploy up to date EMV technology properly; (d) use available technology to defend its POS terminals from well-known methods of invasion; and (e) act reasonably to prevent the foreseeable harms to Plaintiff and the Class which would naturally result from payment card data theft.

52. Defendant negligently allowed payment card magnetic stripe information to be compromised by failing to take reasonable steps against an obvious threat.

53. In addition, in the years leading up to the Noodles data breach, and during the course of the breach itself and the investigation that followed, Noodles failed to follow the guidelines set forth by the FTC. Furthermore, by failing to have reasonable data security measures in place, Noodles engaged in an unfair act or practice within the meaning of §5 of the FTC Act.

54. As a result of the events detailed herein, Plaintiff and members of the Class have been and continue to be forced to protect their customers and avoid fraud losses by cancelling and reissuing cards with new account numbers and magnetic stripe information.

55. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the Class, all of which were proximately caused by Defendant's negligence. As a result of the events detailed herein, Plaintiff and members of the Class suffered losses resulting from the Noodles Data Breach related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as cancelling compromised cards and purchasing and mailing new cards to their customers.

56. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action individually and on behalf of all other financial institutions similarly situated pursuant to Fed. R. Civ. P. 23. The proposed Class is defined as:

> All Financial Institutions − including, but not limited to, banks and credit unions − in the United States (including its Territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card issuing services, whose customers made purchases from Noodles stores from January 1, 2016 to the present (the "Class").

58. Excluded from the Class are Defendants and their subsidiaries, franchises, and affiliates; all employees of Defendants; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

59. Plaintiff is a member of the Class it seeks to represent.

60. The Class is so numerous that joinder of all members is impracticable.

61. The members of the Class are readily ascertainable.

62. Plaintiff's claims are typical of the claims of all members of the Class.

63. The conduct of Defendant has caused injury to Plaintiff and members of the Class in substantially the same ways.

64. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendant.

65. Plaintiff will fairly and adequately represent the interests of the Class.

66. Defendant has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

67. Plaintiff is represented by experienced counsel who are qualified to litigate this case.

68. Common questions of law and fact predominate over individualized questions. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

69. There are questions of law and fact common to all members of the Class, the answers to which will advance the resolution of the claims of the Class members and that include, without limitation:

(a) Whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

(b) Whether the conduct of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

(c) Whether Defendant's actions were negligent;

(d) Whether Defendant owed a duty to Plaintiff and the Class;

(e) Whether the harm to Plaintiff and the Class was foreseeable;

(f) Whether Plaintiff and members of the Class are entitled to injunctive relief; and

(g) Whether Plaintiff and members of the Class are entitled to damages and the measure of such damages.

COUNT ONE
NEGLIGENCE

70. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

71. Defendant owed – and continues to owe – a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and processing Plaintiff's customers' personal and financial information.

72. Defendant owed a duty to Plaintiff and the Class to provide adequate security to protect their mutual customers' personal and financial information.

73. Noodles has a common law duty to prevent the foreseeable risk of harm to others, including the Plaintiff and the Class. It was certainly foreseeable to Noodles that injury would result from a failure to use reasonable measures to protect Payment Card Data and to provide timely notice that a breach was detected. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Payment Card Data belonging to millions of

Noodles customers; thieves would use Payment Card Data to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud by cancelling and reissuing the compromised cards and reimbursing their customers for fraud losses; and that the resulting financial losses would be immense.

74. Noodles assumed the duty to use reasonable security measures as a result of its conduct.

75. Noodles' duty to use reasonable data security measures also arose under §5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Payment Card Data by businesses such as Noodles. The FTC publications and data security breach orders described above further form the basis of Noodles' duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the part of Noodles.

76. Defendant breached its duties by: (1) allowing a third-party intrusion into their computer systems; (2) failing to protect against such an intrusion; (3) failing to maintain updated EMV card systems, updated POS terminals, and secure systems and software necessary to prevent such an intrusion; and (4) allowing the personal and financial information of customers of Plaintiff and the Class to be accessed by third parties on a large scale.

77. Defendant knew or should have known of the risk that its POS terminals could be infiltrated using methods similar or identical to those previously used against major retailers in recent months and years.

78. Defendant knew or should have known that its failure to take reasonable measures

to protect its POS terminals against obvious risks would result in harm to Plaintiff and the Class.

79. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

COUNT TWO
NEGLIGENCE *PER SE*

80. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

81. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Noodles, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of Noodles' duty.

82. Noodles violated §5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Card Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Noodles' conduct was particularly unreasonable given the nature and amount of Payment Card Data it obtained and stored and the foreseeable consequences of a data breach at an international restaurant, including, specifically, the immense damages that would result to consumers and financial institutions.

83. Noodles' violation of §5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

84. Plaintiff and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses.

Moreover, many of the Class members are credit unions, which are organized as cooperatives, whose members are consumers.

85. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 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 harm suffered by Plaintiff and the Class.

86. As a direct and proximate result of Noodles' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT THREE
DECLARATORY AND INJUNCTIVE RELIEF

87. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

88. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

89. An actual controversy has arisen in the wake of the Noodles data breach regarding its common law and other duties to reasonably safeguard Payment Card Data. Plaintiff alleges that Noodles' data security measures were inadequate and remain inadequate. Noodles denies these allegations. Furthermore, Plaintiff continues to suffer injury as additional fraudulent charges are being made on payment cards issued to Noodles customers.

90. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Noodles continues to owe a legal duty to secure its customers' personal and financial information – specifically including information pertaining to credit and debit cards used by Noodles customers – and to notify financial institutions of a data breach under the common law, §5 of the FTC Act, PCI DSS standards, its commitments, and various state statutes;

(b) Noodles continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

(c) Noodles' ongoing breaches of its legal duty continue to cause Plaintiff harm.

91. The Court also should issue corresponding injunctive relief requiring Noodles to employ adequate security protocols, consistent with industry standards, to protect its Payment Card Data. Specifically, this injunction should, among other things, direct Noodles to:

(a) utilize industry standard encryption to encrypt the transmission of cardholder data at the point-of-sale and at all other times;

(b) implement encryption keys in accordance with industry standards;

(c) implement EMV technology;

(d) engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

(e) audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

(f) regularly test its systems for security vulnerabilities, consistent with industry standards;

(g) comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and

(h) install all upgrades recommended by manufacturers of security software and firewalls used by Noodles.

92. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Noodles. The risk of another such breach is real, immediate, and substantial. If another breach at Noodles occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for out of pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable and reputational damage.

93. The hardship to Plaintiff and the Class, if an injunction is not issued, exceeds the hardship to Noodles, if an injunction is issued. Among other things, if another massive data breach occurs at Noodles, Plaintiff and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Noodles of complying with an injunction, by employing reasonable data security measures, is relatively minimal and Noodles has a pre-existing legal obligation to employ such measures.

94. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Noodles, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendant and in favor of Plaintiff and the Class and award the following relief:

A. That this action be certified as a class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as representative of the Class and Plaintiff's counsel as counsel for the Class;

B. Monetary damages;

C. Injunctive relief;

D. Reasonable attorneys' fees and expenses, including those related to experts and consultants;

E. Costs;

F. Pre- and post-judgment interest; and

G. Such other relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff, individually and on behalf of the Class, demands a trial by jury for all issues so triable.

DATED: September 6, 2016

Respectfully submitted,

s/ Joseph P. Guglielmo

Joseph P. Guglielmo
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com

Erin G. Comite
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Telephone: (860) 537-5537
Facsimile: (860) 537-4432
ecomite@scott-scott.com

Gary F. Lynch
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th floor
Pittsburg, PA 15212
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com

Charles H. Van Horn
BERMAN FINK VAN HORN P.C.
3475 Piedmont Road, Suite 1100
Atlanta, GA 30305
Telephone: (404) 261-7711
Facsimile: (404) 233-1943
CVanHorn@bfvlaw.com

Karen H. Riebel
Kate Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter@locklaw.com

Attorneys for Plaintiff SELCO Community Credit Union

CERTIFICATE OF SERVICE

I hereby certify that on September 6, 2016, a copy of the foregoing was filed electronically and served by mail on anyone unable to accept electronic filing. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing.

I certify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on September 6, 2016.

s/ Joseph P. Guglielmo
Joseph P. Guglielmo
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com