UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

MICHAL FUS, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	No.
v.	)	JURY TRIAL DEMANDED
CAFEPRESS, INC.,	)	
Defendant.	)	

COMPLAINT

Plaintiff Michal Fus, individually and on behalf of all others similarly situated, by and through his attorneys, Fegan Scott LLC, for their Complaint against Defendant CafePress, Inc., allege as follows:

I. INTRODUCTION

1. CafePress is heralded as the world's largest online gift shop, carrying more than one billion products on its website, including t-shirts, mugs, and bags that can be user-customized with logos and other designs. Tens of millions of people have trusted CafePress with their online shopping, which CafePress touts as: "Safe and Secure Shopping. Guaranteed."

2. Despite its guarantee, on October 2, 2019, CafePress notified its customers that its online shopping website database had been hacked nine months earlier in February of 2019.

3. CafePress failed to protect Plaintiff's and its customers' personal information, including their names, addresses, telephone numbers, email addresses, passwords, the last four digits of credit cards, credit card expiration dates, and, in some instances, social security numbers and tax identification numbers.

4. Since the data breach occurred, CafePress customers have been exposed to credit

card theft and subjected to resulting economic losses. Plaintiff has and will incur costs to mitigate the risk for the data breach, such as paying for credit monitoring services. Regardless of whether they have yet to incur out-of-pocket losses, Plaintiff and all CafePress customers whose personal information was stolen remain subject to a pervasive, substantial and imminent risk of identity theft and fraud.

5. This class action is brought on behalf of all natural persons victimized by the CafePress data breach to redress the damage that they have suffered and to obtain appropriate equitable relief to mitigate the risk that CafePress will allow another breach in the future. Plaintiff and the nationwide class he seeks to represent assert claims for CafePress's negligence, negligence per se, and violations of state consumer protection laws.

II. JURISDICTION

6. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000 and Defendant is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in this District and CafePress does business in this District and is therefore subject to personal jurisdiction in this District.

III. PARTIES

8. Plaintiff Michal Fus is a resident and citizen of the State of Illinois (DuPage

County) whose Personal Information[1] was compromised in the Defendant CafePress, Inc.'s data breach. Plaintiff received a notice on October 2, 2019 from CafePress that his Personal Information was compromised. Plaintiff has and will spend time and money employing a credit monitoring service and putting credit freezes in place to mitigate possible harm. In addition, as a result of the breach, Plaintiff will spend time and effort making multiple telephone calls to his bank and credit card company, monitoring his financial accounts, searching for fraudulent activity, and reviewing his credit reports. Plaintiff would not have purchased products from CafePress's website had he known of its inadequate data security practices. Given the nature of the information stolen, Plaintiff remains at a substantial and imminent risk of future harm.

9. Defendant CafePress, Inc. is a Delaware corporation with its principal place of business located at 11909 Shelbyville Road, Louisville, Kentucky. CafePress sells merchandise on its website, www.cafepress.com, and ships merchandise nationwide, including to Illinois.

10. During the check-out process on its website, CafePress customers are never asked to agree to or to read any particular terms and conditions as part of the sale. CafePress does not show any terms or conditions in a customer's online cart or at the time of purchase when inputting payment information. Rather, the check-out process is akin to a brick-and-mortar store where customers can make purchases without agreeing to any limits of liability, waivers or arbitration provisions.

IV. FACTS

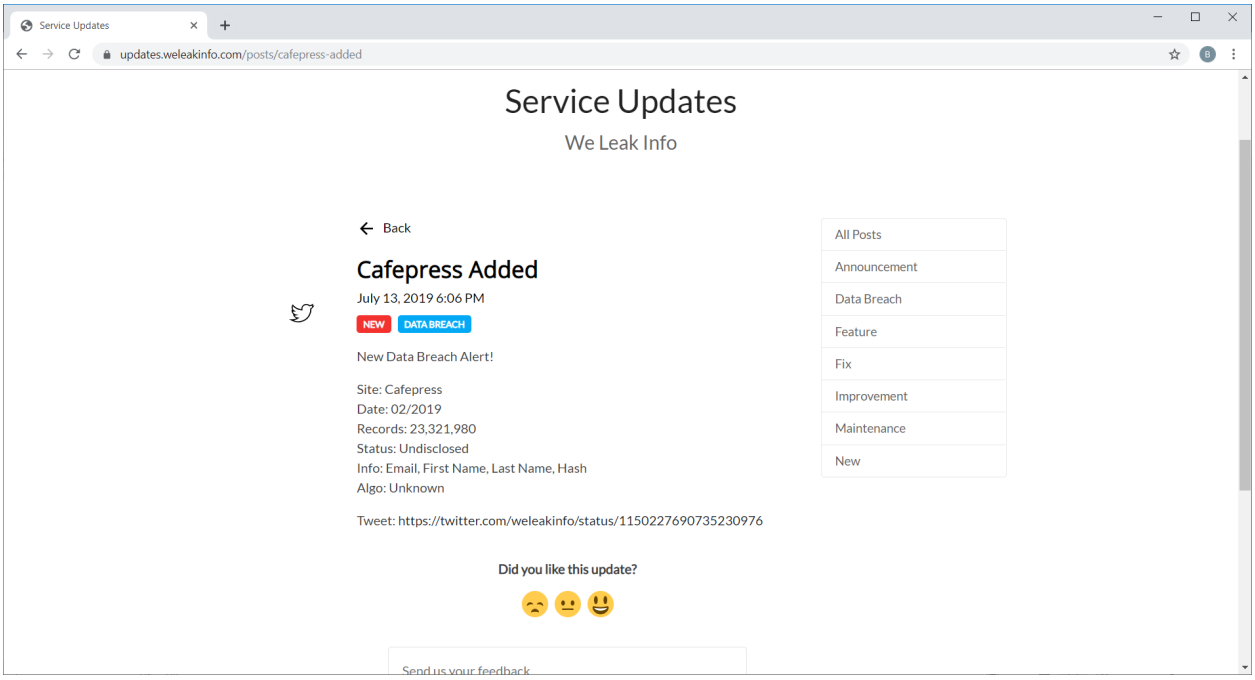
11. On or about February 20, 2019, CafePress's online databases were hacked and

[1] As used throughout this Complaint, "Personal Information" is defined as all information exposed by the CafePress data breach, including but not limited to all or any part or combination of name, address, telephone number, date of birth, email address, password, credit card number, credit card expiration date, social security number, tax identification number, and other personally identifying information.

data for a total of 23,205,290 accounts was exposed. The breached data included 23 million unique email addresses, passwords, names, physical addresses, phone numbers, the last for digits of credit cards, credit card expiration dates, and in some instances, social security numbers.

12. Yet, due to apparently lax security protocols, CafePress either did not discover the breach of its databases or took steps to hide the breach from its customers.

13. On or about July 13, 2019, a website titled We Leak Info reported that CafePress had suffered a data breach:

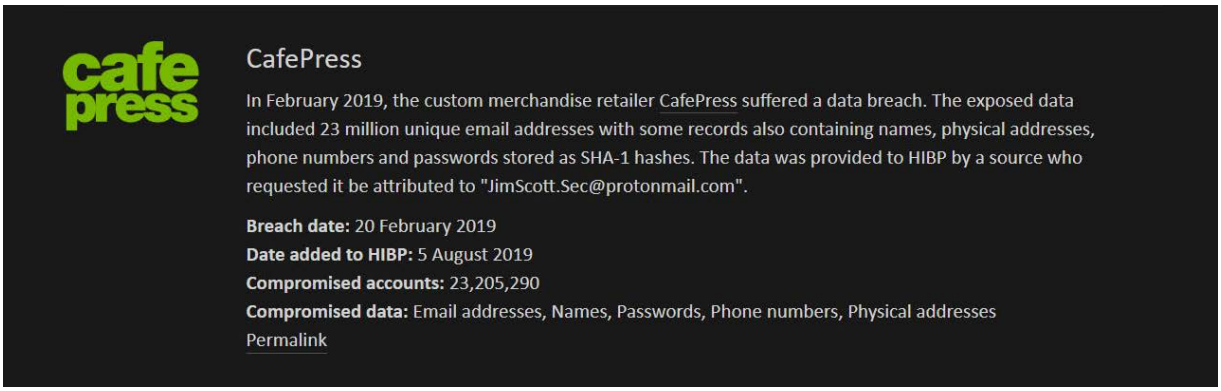


14. Yet, CafePress did not take any steps to notify its customers of the breach.

15. On or about August 5, 2019, a second breach database service, haveibeenpwned (HIBP), reported the data breach. Created by a Microsoft Regional Director, HIBP is a free online resource for anyone to quickly assess if they may have been put at risk due to an online account having been compromised or "pwned" in a data breach.

16. HIBP reported that it had received a tip that “exposed data included 23 million

unique email addresses with some records also containing names, physical addresses, phone numbers and passwords stored as SHA-1 hashes. The data was provided to HIBP by a source who requested it be attributed to 'JimScott.Sec@protonmail.com'." An excerpt from the website follows:



17. Designed by the United States National Security Agency, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input (such as a password) and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long.

18. Since 2005, SHA-1 has not been considered secure against hackers. Since 2010, many organizations have recommended its replacement by SHA-2 or SHA-3.

19. Nonetheless, according to HIBP, CafePress continued to store some of its customers' personal-identifying information using SHA-1.

20. Also, on August 5, 2019, *Forbes* published an article entitled, "CafePress Hacked, 23M Accounts Compromised. Is Yours One of Them?" *Forbes* (8/5/19).[2]

21. *Forbes* reported that the breach compromised a total of 23,205,290 accounts, and

[2] *See* https://www.forbes.com/sites/daveywinder/2019/08/05/cafepress-hacked-23m-accounts-compromised-is-yours-one-of-them/#155278bf407e (last visited 10/2/19).

the exposed data included 23 million unique email addresses, names, physical addresses, phone numbers, and passwords, roughly half of which were "encoded in a base64 SHA1, which is a very weak encryption method to use especially in 2019 when better alternatives are available."

22. According to *Forbes*, a CafePress spokesperson stated: "CafePress Inc. learned of a potential security issue related to customer accounts. We have engaged third-party experts and are investigating the issue. Our commitment to maintaining the confidentiality of our customers' information is paramount to the employees and leadership of CafePress."

23. Yet, CafePress did not take steps to notify its customers whose personal-identifying information was compromised.

24. During that same month, August of 2019, CafePress forced users to change their passwords but claimed it was due to a policy update.[3] Again, CafePress did not notify its customers of the data breach, and, in fact, attempted to conceal the reason why it was requiring its customers to change their passwords.

25. CafePress's website, updated on September 5, 2019, a month before it contacted its customers, acknowledged the hacking. The website states that the data breach affected "approximately 22 million customer accounts in the United States and globally," and "included names, email addresses, passwords to customer CafePress accounts, and other information" and "the information also included Social Security Numbers or Tax Identification Numbers" for less than 1% of those affected individuals. https://www.cafepress.com/p/security2019 (last visited 10/2/19).

26. Finally, on or about October 2, 2019, Plaintiff and other CafePress customers

[3] *See* "CafePress Informs Customers of Massive February Data Hack," *Advertising Specialty Institute,* found at https://www.asicentral.com/news/newsletters/promogram/september-2019/cafepress-informs-customers-of-massive-february-data-hack/ (last visited 10/2/19) (attribution omitted).

received an email, notifying them of a "data security incident" involving their personal information, which "may have occurred on or about February 19, 2019." This was the first time Plaintiff learned his information was subject to the data breach.

27. The email from CafePress stated that it "recently discovered" that "an unidentified third party" "may have obtained customer information…contained in a CafePress database," and that the data theft "may have included" their "name, email address, the password to [their] CafePress account, and other information."

28. CafePress advised Plaintiff to "remain vigilant and take steps to protect against identify theft or fraud, including monitoring your accounts and free credit reports for signs of suspicious activity;" "visit the CafePress website… and change your account password;" and contact the credit reporting agencies (CRAs), Experian, TransUnion and Equfax, "to place a 'fraud alert' on your credit file." *Id.* The CafePress email cautioned customers that "security freezes" are available from the CRAs, but that "placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services."

29. The CafePress data breach has forced and will force consumers to spend time and money to protect themselves, including purchasing credit monitoring services and implementing account protections, such as a credit or security "freezes."

30. Yet as CafePress's October 2, 2019 email noted, while a security freeze allows a consumer to restrict access to their credit report, which in turn makes it more difficult for identity thieves to open new accounts in that consumer's name, they can create barriers for consumers who are quickly in need of credit.

31. Experian's website confirms these difficulties and challenges of freezing credit.[4] Experian acknowledges that, "Credit freezes can create delays and problems when credit is needed quickly in the case of applying for a loan, credit card, or even a job hunt…. During a freeze period, most companies will not extend credit until they check one's credit file with one or three major credit bureaus, and that takes time." *Id.*

32. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

33. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

[4] https://www.experian.com/blogs/ask-experian/7-things-you-need-to-know-before-freezing-your-credit/ (last visited 10/2/19).

34. Consequently, victims of the Defendant's data breach are at an imminent risk of fraud and identity theft now and for years to come.

35. Defendant's actions and failures to act when required have caused Plaintiff and the Class harm and/or the significant and imminent risk of future harm, including:

a. theft of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals; and

h. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and the Class.

V. CLASS ACTION ALLEGATIONS

36. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff seeks certification of the following nationwide class: "All persons residing in the United States whose

Personal Information was compromised in the CafePress, Inc. data breach that occurred in February, 2019."

37. Plaintiff also seeks certification, pursuant to Rule 23(b)(2) and (b)(3) of the following Illinois Subclass: "All persons residing in Illinois whose Personal Information was compromised in the CafePress, Inc. data breach that occurred in February, 2019."

38. ***Numerosity***: ***Federal Rule of Civil Procedure 23(a)(1).*** The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. CafePress has revealed that over 22 million customer accounts in the United States and globally have been affected, making joinder impracticable. Those individuals' names and addresses are available from Defendant's records, and Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

39. ***Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).*** This action involves common questions of law and fact, which predominate over any questions affecting individual class members, including:

a. Whether Defendant knew or should have known that its computer systems were vulnerable to attack;

b. Whether Defendant failed to take adequate and reasonable measures to ensure its data systems were protected;

c. Whether Defendant failed to take available steps to prevent and stop the breach from happening;

d. Whether Defendant failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard its customers' Personal Information;

e. Whether Defendant failed to provide timely and adequate notice of the data breach;

f. Whether Defendant owed a duty to Plaintiff and Class members to protect their Personal Information and to provide timely and accurate notice of the

data breach to Plaintiff and Class members;

g. Whether Defendant breached its duties to protect the Personal Information of Plaintiff and Class members by failing to provide adequate data security and by failing to provide timely and accurate notice to Plaintiff and Class members of the data breach;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unauthorized access and/or theft of consumers' Personal Information;

i. Whether Defendant's conduct violated state consumer protection laws;

j. Whether Defendant's conduct renders it liable for negligence, negligence per se, or unjust enrichment;

k. Whether, as a result of Defendant's conduct, Plaintiff and Class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

l. Whether, as a result of Defendant's conduct, Plaintiff and Class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief; and

m. Whether, as a result of Defendant's conduct, Plaintiff and Class members are entitled to damages, punitive damages, costs, and attorneys' fees.

40. ***Typicality: Federal Rule of Civil Procedure 23(a)(3).*** Plaintiff's claims are typical of other Class members' claims because Plaintiff and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

41. ***Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).*** Plaintiff is an adequate class representative because his interests do not conflict with the interests of Class members who he seeks to represent, Plaintiff has retained counsel competent and experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and his counsel.

42. ***Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).***

The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

43. ***Superiority: Federal Rule of Civil Procedure 23(b)(3).*** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court, especially where by CafePress's own admission, there are over 22 million customers affected.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

44. Individually and on behalf of the Nationwide Class, Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

45. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care

in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class members' Personal Information in its possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with current technology and industry standards.

46. Defendant's duty to use reasonable care arose from several sources. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiff and other Class members would be harmed.

47. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, 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 Personal Information by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

48. Timely notification of the data breach was required, appropriate and necessary so that, among other things, Plaintiff and Class members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct.

49. Defendant breached the duties it owed to Plaintiff and Class members described above and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with current technology and industry standards; and (d) timely disclose that Plaintiff's and the Class members' Personal Information in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

50. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their Personal Information would not have been compromised.

51. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Plaintiff's and Class members' injuries include:

a. theft of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach— including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals; and

h. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class members.

COUNT II
NEGLIGENCE PER SE

52. Individually and on behalf of the Nationwide Class, Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

53. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Defendant of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Defendant's duty.

54. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information, failing to use current and generally accepted technology, and not complying with industry standards. Defendant's conduct was particularly unreasonable given the size of its customer database, the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach.

55. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

56. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

57. Moreover, 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 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 harm suffered by Plaintiff and the Class.

58. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
ILLINOIS PERSONAL INFORMATION PROTECTION ACT, 815 ILL. COMP. STAT. §§ 530/10(A), *ET SEQ.*

59. Individually and on behalf of the Illinois Subclass, Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

60. As a corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information, Defendant is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

61. Plaintiff and Illinois Subclass members' Personal Information (e.g., Social Security numbers) includes Personal Information as covered under 815 Ill. Comp. Stat. § 530/5.

62. As a Data Collector, Defendant is required to notify Plaintiff and Illinois Subclass members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

63. By failing to disclose the data breach in the most expedient time possible and without unreasonable delay, Defendant violated 815 Ill. Comp. Stat. § 530/10(a).

64. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

65. As a direct and proximate result of Defendant's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Illinois Subclass members suffered damages, as described above.

66. Plaintiff and Illinois Subclass members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Defendant's willful conduct.

COUNT IV

ILLINOIS CONSUMER FRAUD ACT, 815 ILL. COMP. STAT. §§ 505, *ET SEQ.*

67. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein on behalf of the Illinois Subclass.

68. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

69. Plaintiff and Illinois Subclass members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

70. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

71. Defendant's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Defendant data breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Defendant data breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Personal Information; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

72. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

73. Defendant intended to mislead Plaintiff and Illinois Subclass members and induce

them to rely on its misrepresentations and omissions.

74. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

75. Defendant acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass members' rights.

76. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

77. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT V

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILL. COMP. STAT. §§ 510/2, *ET SEQ.*

78. Individually and on behalf of the Illinois Subclass, Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

79. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

80. Defendant engaged in deceptive trade practices in the conduct of its business, in

violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

81. Defendant's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Defendant data breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Defendant data breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Personal Information; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information.

82. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

83. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

84. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

85. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

WHEREFORE, Plaintiff respectfully requests that this Court:

a. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's counsel as Class Counsel;

b. Grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. Award Plaintiff and Class members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

d. Award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

e. Grant declaratory relief sought herein;

f. Award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

g. Award pre- and post-judgment interest at the maximum legal rate; and

h. Grant all such other relief as is just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Dated: October 4, 2019

FEGAN SCOTT LLC

By: */s/ Elizabeth A. Fegan*

Elizabeth A. Fegan
Timothy A. Scott
FEGAN SCOTT LLC
150 S. Wacker Dr., 24th Floor
Chicago, IL 60606
Phone: 312.741.1019
Fax: 312.264.0100
beth@hbsslaw.com
tim@feganscott.com

Lynn A. Ellenberger
FEGAN SCOTT LLC
500 Grant St., Suite 2900
Pittsburgh, PA 15219
lynn@feganscott.com

Counsel for Plaintiff