UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

JEFFREY JACOBS, individually and on behalf of all others similarly situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., and CAPITAL ONE BANK (USA), N.A., Defendants.	Civil Action No. 1:19-cv-03217 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jeffrey Jacobs, individually and on behalf of all others similarly situated, by counsel, hereby brings the present action against Defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A., and in support thereof specifically alleges as follows:

SUMMARY OF THE CASE

1. Every business that collects and stores sensitive information about its customers has a duty to safeguard that information and ensure it is secure and remains private. That responsibility is most important where a business keeps and stores highly personal data such as the Social Security numbers and financial information belonging to its customers.

2. The data collected and stored by financial institutions are among the most highly sensitive personally identifiable information. These companies, in turn, bear the crucial responsibility to protect this data from compromise and theft.

3. Defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A. (collectively, "Capital One" or "Defendants") comprise one of the largest credit card issuers in the United States. Accordingly, Defendants maintain a massive amount of PII on their past and current cardholders, as well as consumers who applied for, but ultimately were not issued, payment cards. Defendants have common law and statutory duties to take reasonable and appropriate measures to protect these consumers' sensitive information and to safeguard it from theft.

4. This lawsuit arises from Defendants' failure to fulfill their legal duties to protect the personal information of more than 100 million consumers and small businesses whose data was stored in Defendants' systems. The compromised records include consumers' names, Social Security numbers, addresses, phone numbers, email addresses, dates of birth, bank account numbers, fragments of transaction history, payment history, self-reported income, and credit scores (collectively "Sensitive Information"). This breach is the result of Defendants' failure to implement data security measures commensurate with the duties they undertook by storing vast quantities of Sensitive Information.

5. Defendants have yet to fully and accurately inform those affected of the scope of the compromise or the nature of the risks associated with identity theft. It is unclear how many victims, if any, Defendants have personally notified.

6. This delay in notification is unacceptable as, in a data breach situation, it is incumbent upon the breached company to provide accurate and complete information to those at risk so they may immediately move to protect themselves and their families from further harm.

7. In short, Defendants breached their duties to protect and safeguard their customers' Sensitive Information.

8. Plaintiff brings this action for himself and on behalf of all persons similarly situated, whose Sensitive Information was stored by Defendants and compromised as a result of Defendants' failure to safeguard that information. Because Defendants failed in their duty to protect the information of more than 100 million consumers, they must stand to account before the law.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiff is a citizen of Indiana and the proposed class members are from various states, while Defendants are citizens of Virginia; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

10. This Court has personal jurisdiction over Defendants because Defendants conduct business in and throughout the Southern District of Indiana.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

PARTIES

12. Plaintiff Jeffrey Jacobs is an individual residing in Richmond, Indiana who is a Capital One credit card holder and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

13. Defendant Capital One Financial Corporation is a Delaware corporation with its principal place of business in McLean, Virginia.

14. Defendant Capital One, N.A., is a national bank with its principal place of business in McLean, Virginia. Defendant Capital One, N.A. is a wholly-owned subsidiary of Capital One Financial Corporation.

15. Defendant Capital One Bank (USA), N.A., is a national bank with its principal place of business in McLean, Virginia. Defendant Capital One Bank (USA), N.A. is a wholly-owned subsidiary of Capital One Financial Corporation.

FACTUAL BACKGROUND

A. The Data Breach

16. Defendant Capital One Financial Corporation, through its subsidiaries, including Defendants Capital One, N.A., and Capital One Bank (USA), N.A., is one of the largest credit-card issuers in the United States, and one of the top 10 largest banks based on deposits.

17. On July 29, 2019, Capital One publicly announced that a hacker had breached its systems and "obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers." [1] The announcement noted that Capital One had discovered the Data Breach on July 19, 2019 and estimated that "approximately 100 million individuals in the United States and approximately 6 million in Canada" were affected.[2]

18. Capital One further disclosed that the breached Sensitive Information included customers' names, addresses, zip codes, postal codes, phone numbers, email addresses, dates of birth, self-reported income, credit scores, credit limits, balances, payment history, contact information, and fragmented transactional data. Capital One also stated that the breach

[1] Capital One Announces Data Security Incident, Capital One, http://phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irol-newsArticle_Print&ID=2405042 (emphasis added) (last accessed July 30, 2019).
[2] *Id.*

compromised approximately 80,000 linked bank account numbers of secured credit card customers.

19. The Data Breach occurred on March 22 and 23, 2019, but went undiscovered by Defendants for nearly four months. On July 19, 2019, Defendants finally discovered that the Sensitive Information of over 100 million customers and credit card applicants had been breached.

20. Capital One learned of the Data Breach after an individual previously unknown to Defendants emailed them a link to a file containing the leaked Sensitive Information. The file provided in the link was timestamped April 21, 2019 and included code for commands used in the Data Breach, as well as a list of more than 700 folders or buckets of data.

21. As this email evinces, the hacker seemingly had unfettered access to the massive amount of Sensitive Information stored on Capital One's systems at least until April 21, 2019.

22. Defendants promised credit card applicants and customers like Plaintiff and Class members that it would protect the Sensitive Information entrusted to it. As one example, Capital One's Privacy Policy promises that Capital One will "protect your personal information from unauthorized access and use" and represents that it will only share customers' Sensitive Information for a short list of enumerated reasons.[3]

23. Capital One's online credit card applications also explicitly promise customers that Capital One will keep their Sensitive Information confidential and will protect it against unauthorized access and use, stating that "Capital One uses 256-bit Secure Sockets Layer (SSL)

[3] *Privacy Policy*, Capital One, https://www.capitalone.com/bank/privacy/ (last accessed July 30, 2019).

technology. This means that when you are on our website, the data transferred between Capital One and you is encrypted and cannot be viewed by any other party."[4]

24. Industry standards also require Capital One to keep its customers' Sensitive Information confidential and to protect it from unauthorized disclosures.

25. Plaintiff and Class members provided their Sensitive Information to Capital One with the understanding that Capital One would comply with their promises and obligations to keep their Sensitive Information confidential and to protect it against unauthorized disclosures.

26. Defendants' security failures demonstrate that they breached their duties and promises to protect customers' Sensitive Information by failing to:

a. maintain an adequate data security system to protect Sensitive Information against unauthorized access, disclosure, or use;

b. adequately monitor its system to identify unauthorized access, disclosure, or use of the Sensitive Information stored therein;

c. timely and adequately discover when and how customers' Sensitive Information was accessed, disclosed, or used without proper authorization during the Data Breach;

d. timely and adequately discover the amount and type of Sensitive Information that was accessed, disclosed, or used without proper authorization; and

e. timely and adequately notify Plaintiff and Class members of the Data Breach.

[4] *E.g.*, Application for Platinum Credit Card, https://applynow.capitalone.com/?productId=6675# (last accessed July 31, 2019) (emphasis added).

27. Plaintiff and members of the Classes have been injured by the unauthorized access and disclosure of their Sensitive Information in the Data Breach.

B. The Value of Stolen Data

28. The breadth of data compromised in the Capital One Data Breach is astounding and the highly sensitive nature of the information makes it particularly valuable to thieves. The compromised data leaves Defendants' customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more. As Pam Dixon, executive director of the World Privacy Forum, stated: "When someone has . . . your bank account information[] and your Social Security number, they can commit fraud that lasts a long time. Th[is] kind of identity theft . . . is qualitatively and quantitatively different than what is typically possible when you lose your credit card . . . ."[5]

29. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

30. The Social Security Administration has warned that identity thieves can use an individual's Social Security number and good credit score to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[6]

31. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of

---

[5] Jaikumar Vijayan, *Premera Hack: What Criminals Can Do With Your Healthcare Data*, Christian Science Monitor (Mar. 20, 2015), http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data.

[6] Social Security Administration, Identity Theft and Your Social Security Number, http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 31, 2019).

these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

32. It is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

33. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[7]

34. The personal information compromised in the Capital One Data Breach is significantly more valuable than the unauthorized access and disclosure of credit card information affected in the large retailer data breaches at Target and Home Depot. Victims affected by the retailer breaches could avoid much of the potential for future harm by cancelling credit or debit cards and obtaining replacements. The information compromised in the Capital One breach—Social Security number, name, date of birth, employment information, income data, etc.—is difficult, if not impossible, to change.

35. Criminals who access individuals' Sensitive Information can empty a victim's bank account or commit numerous types of identity fraud, including obtaining a driver's license

[7] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Sept. 16, 2015).

or official identification card in the victim's name but with the thief's picture, using the victim's name and Social Security number to obtain government benefits, renting a house, or receiving medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[8]

36. Because this Sensitive Information is so valuable to identity thieves, information compromised during data breaches are often traded on the black market for years. This Sensitive Information, as one would expect, demands a much higher price on the black market than other data, such as credit card numbers. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[9]

37. The implications of the Capital One Data Breach are indeed serious. But these implications were publicized and were known to Capital One well before the Data Breach actually occurred. Defendants should have—and could have—done more to fulfill their duty to safeguard the Sensitive Information with which they were entrusted.

38. Defendants have had multiple security breaches in the past and thus Capital One had ample warnings of weaknesses and risks to its systems. For example, on or about January 2018, Capital One suffered a data breach that compromised 50GB worth of sensitive data. Capital One has also issued letters on or about on or about November 2014, July 28, 2017, July 31, 2017, and September 12, 2017 that notified an undisclosed number of customers that their personal information may have been compromised during other data breaches.

---

[8] See *Warning Signs of Identity Theft*, Federal Trade Commissions, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed July 29, 2019).
[9] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

CLASS ALLEGATIONS

39. In accordance with Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), Plaintiff brings this case individually and as a class action on behalf of two classes of consumers (collectively "the Classes") defined as follows:

> All persons in the United States whose Sensitive Information was maintained on Capital One's systems and was compromised by the data breach announced by Capital One on July 29, 2019 (The "Nationwide Class")
>
> All citizens of Indiana whose Sensitive Information was maintained on Capital One's systems and was compromised by the data breach announced by Capital One on July 29, 2019 (The "Indiana Class")

40. Excluded from the Classes are: (1) Defendants, any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded, divided into subclasses, or modified in any other way.

41. **Numerosity.** The Classes are so numerous that joinder of all members is impracticable. On information and belief, the Nationwide Class includes more than 100 million members whose Sensitive Information was compromised by the Data Breach. Upon information and belief, the Indiana Class includes thousands of similarly-situated individuals whose Sensitive Information was compromised by the Data Breach. Disposition of the claims of these Classes in a single action will provide substantial benefits to all parties and to the Court. Class membership

is readily identifiable from information and records in Defendants' possession, custody, or control.

42. **Typicality.** Plaintiff's claims are typical of the claims of the Classes in that Plaintiff, like all Class members, entrusted his Sensitive Information to Capital One and suffered the same injury as all Class members, namely that, upon information and belief, his Sensitive information was compromised in the Data Breach. Further, the factual bases of Defendants' misconduct are common to all Class members and represent a common thread of misconduct resulting in injury to all Class members.

43. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent legal counsel with significant experience in complex and class action litigation, including consumer and data breach class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to or that conflict with those of the proposed Classes.

44. **Predominance of Common Issues.** There are numerous questions of law and fact common to Plaintiff and the Classes that predominate over any questions affecting only individual Class members. The answers to these common questions will advance resolution of the litigation as to all Class members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants owed a duty to Plaintiff and the Classes to take reasonable measures to safeguard their Sensitive Information;

b. Whether Defendants knew or should have known that the data security systems maintaining customers' Sensitive Information were vulnerable to attack;

c. Whether Defendants breached their legal duties in allowing their data security systems to be compromised, permitting unauthorized access to over 100 million individual files;

d. Whether Defendants owed a duty to Plaintiff and the Classes to provide timely and adequate notice of the Data Breach and the risks posed thereby, and whether Defendants' notice was, in fact, timely;

e. Whether Defendants' data security systems prior to the Data Breach complied with all applicable legal requirements;

f. Whether Defendants' data security systems prior to the Data Breach met industry standards;

g. Whether Plaintiff and other Class members' Sensitive Information was compromised in the Data Breach; and

h. Whether Plaintiff and other Class members are entitled to damages as a result of the Data Breach.

45. **Superiority.** Plaintiff and members of the Classes have all suffered and will continue to suffer harm and damages as a result of Defendants' unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

46. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Further,

without class litigation, Class members will continue to incur damages, and Defendants are likely to repeat their misconduct.

47. Class treatment of common questions of law and fact is also a superior method for litigating multiple individual actions in that class treatment will conserve the resources of the courts and the litigants and will promote consistency and efficiency of adjudication.

48. Plaintiff does not anticipate any management difficulties.

CAUSES OF ACTION

COUNT ONE
Negligence
(Individually and On Behalf of the Classes)

49. Plaintiff realleges and incorporates by reference all preceding factual allegations.

50. Capital One required Plaintiff and Class Members to submit their Sensitive Information when applying for a credit card. Defendants thus collected and maintained a massive amount of Sensitive Information.

51. By collecting and maintaining this Sensitive Information, and by using and sharing it for commercial gain, Defendants assumed duties of care to use reasonable means to secure and safeguard this Sensitive Information, to prevent unauthorized access to or disclosure of this Sensitive Information, and to protect this Sensitive Information from theft.

52. Defendants' duties included a responsibility to implement reasonable technical, administrative, and physical security measures that would permit them to detect, respond to, remedy, and notify affected individuals of security breaches in a reasonably expeditious period of time.

53. Defendants also owed a duty of care to Plaintiff and the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to

ensure that their systems and networks—and the personnel responsible for them—adequately protected their customers and potential customers' Sensitive Information.

54. Defendants alone were in a position to ensure that their systems were sufficient to protect Plaintiff and the Classes from the harms associated with a data breach.

55. Defendants breached their duties of care by failing to secure and safeguard the Sensitive Information of Plaintiff and the Classes. Defendants negligently maintained systems that were vulnerable to a security breach and Defendants knew or should have known of these vulnerabilities.

56. Defendants breached their duties of care by failing to adequately implement, monitor, or maintain their data security systems and networks. In fact, Defendants' data security systems were so poorly implemented, monitored, and maintained that the hacker was able to remain undetected in Defendants' systems, allowing her seemingly unfettered access to Plaintiff and the Classes' Sensitive Information for nearly four months.

57. Defendants breached their duties of care by allowing unauthorized access to Plaintiff and Class members' Sensitive Information and by failing to recognize in a timely manner that Plaintiff and other Class members' Sensitive Information had been compromised. Defendant's negligence was such that they were first alerted to the Data Breach when they received an email with a link to a file containing the leaked Sensitive Information as well as hundreds of folders or buckets of data.

58. Given the risks associated with data theft, Defendants also assumed a duty of care to promptly and fully notify and inform individuals affected by a breach should their personal information be compromised and/or stolen.

59. Defendants breached this duty of care when they failed to timely notify the affected individuals of the Data Breach.

60. It was foreseeable that Defendants' failure to use reasonable measures to maintain, protect, and monitor the security of Sensitive Information could result in a security breach and would cause injury to Plaintiff and the members of the Classes.

61. It was also foreseeable that Defendants' failure to adequately safeguard Plaintiff and Class members' Sensitive Information would result in injuries, including but not limited to:

a. ongoing, imminent, and certainly impending threat of identity theft, fraud, and abuse resulting in monetary loss and economic harm;

b. actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;

c. loss of the confidentiality of the stolen data;

d. the illegal sale of the compromised data on the deep web black market;

e. expenses and/or time spent on credit monitoring and identity theft insurance;

f. time spent scrutinizing bank statements, credit card statements, and credit reports;

g. expenses and/or time spent initiating fraud alerts;

h. decreased credit scores and ratings;

i. lost work time; and

j. other economic and non-economic harm.

62. Plaintiff and the Classes have suffered one or more of these harm as a result of Defendants' breach and will continue to be harmed and incur damages both in an effort to protect themselves and to remedy acts of fraudulent activity.

COUNT TWO
Negligence Per Se
(Individually and On Behalf of the Classes)

63. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

64. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to safeguard personal information.

65. Various FTC publications and orders also form the basis of Capital One's duty.

66. Capital One violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff and Class members' Sensitive Information, and by failing to comply with industry standards.

67. Capital One's violation of Section 5 of the FTC Act constitutes negligence per se.

68. Class members are consumers within the class of persons that Section 5 of the FTC Act was intended to protect.

69. The harm resulting from Capital One's conduct is the type of harm the FTC Act was intended to guard against.

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

COUNT THREE
Breach of Implied Contract
(Individually and On Behalf of the Classes)

71. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

72. When Plaintiff and Class members paid money and provided their Sensitive Information to Defendants in exchange for financial services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect their Sensitive Information and to timely and accurately notify them if a data breach occurred and their information was compromised.

73. Defendants solicited and invited prospective clients and other consumers to provide their Sensitive Information as part of its regular business practices. Plaintiff and Class members accepted Defendants' offers and provided their Sensitive Information to Defendants.

74. In entering into such implied contracts, Plaintiff and the Classes assumed that Defendants' data security practices and policies were reasonable and consistent with industry standards, and that Defendants would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices. This assumption was reinforced by Defendant's representations that Capital One would protect customers' Sensitive Information.

75. Plaintiff and the Class would not have provided and entrusted their Sensitive Information to Defendants if not for the implied contract between them and Defendants to keep the information secure.

76. Plaintiff and the Class performed all, or substantially all, of their obligations under the implied contracts with Defendants.

77. Defendants breached their implied contracts with Plaintiff and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of the Data Breach.

78. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiff and the Classes were harmed and incurred damages as described herein.

COUNT FOUR
Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-1, *et seq.*
(Individually and On Behalf of the Indiana Class)

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. As set forth in the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-2, Plaintiff and members of the Indiana Class members are persons who engaged in consumer transactions with Defendants, which are suppliers, for financial services.

81. Defendants represented that the financial services they sold to Plaintiff and members of the Indiana Class members were of a particular standard, quality, grade, style, or model when in fact they were not and Defendant knew or should have reasonably known that they were not.

82. Defendants' conduct as alleged in this Complaint violated Indiana Code § 24-5-0.5-3(b)(1), (2), by:

a. falsely representing to Plaintiff and members of the Indiana Class that Sensitive Information provided to Defendants would be safe and secure from theft and unauthorized disclosure;

b. falsely representing to Plaintiff and members of the Indiana Class that Defendants maintained policies and practices sufficient to secure and safeguard this Sensitive Information;

c. failing to take reasonable means to secure and safeguard this Sensitive Information to prevent the disclosure of the information and to guard it from theft;

d. maintaining systems that Defendants knew were vulnerable to a security breach;

e. failing to implement data security measures commensurate with the duties they undertook by storing vast quantities of Sensitive Information;

f. failing to implement a process by which Defendants could detect a breach of their security systems in a reasonably expeditious period of time;

g. delaying disclosure of the Data Breach; and

h. continuing to collect and maintain Sensitive Information when Defendants knew or should have known of the security vulnerabilities that were exploited in the Data Breach.

83. Plaintiff and members of the Indiana Class relied on Defendants' misrepresentations.

84. Defendants' deceptive acts were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under Indiana Code § 24-5-0.5-1, *et seq*.

85. Plaintiff and the Indiana Class members are entitled to $1,000 or treble damages, reasonable attorneys' fees, costs of suit, and any other relief which the Court deems proper.

RELIEF REQUESTED

WHEREFORE, Plaintiff and Class members demand judgment as follows:

A. An order certifying the proposed Classes, designating Plaintiff as the named representative of the Classes, and designating the undersigned as Class Counsel;

B. An order awarding Plaintiff and the Classes relief, including actual and statutory damages;

C. Any additional orders or judgments as may be necessary to prevent further unlawful practices and to restore to any person in interest any money or property that may have been acquired by means of the violations;

D. An award of attorneys' fees and costs, as provided by law;

E. An award of pre-judgment interest and post-judgment interest, as provided by law;

F. Such other favorable relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of all those similarly situated, hereby requests a jury trial on all claims so triable.

Dated: August 1, 2019

Respectfully submitted,

s/Richard E. Shevitz

Richard E. Shevitz
Lynn A. Toops
Lisa M. La Fornara
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Fax: (317) 636-2593
rshevitz@cohenandmalad.com
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

Counsel for Plaintiff and the Proposed Classes