UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

MICHELLE PROVOST, individually and on behalf of all others similarly situated,	§	
Plaintiff,	§	CIVIL ACTION NO. : _____
v.	§	CLASS ACTION COMPLAINT
APTOS, INC., and TEMPUR SEALY INTERNATIONAL, INC.,	§	**JURY TRIAL DEMANDED**
Defendants.	§	

Plaintiff Michelle Provost, ("Provost" or "Plaintiff"), individually and on behalf of all others similarly situated, alleges the following against Aptos, Inc., ("Aptos") and Tempur Sealy International, Inc. ("Tempur Sealy," and collectively with Aptos, "Defendants") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

SUMMARY OF ACTION

1. This action seeks redress for Defendant's failure to secure and safeguard their customers' personal information, including credit and debit card information and to disclose the extent of the breach of that information and notify affected consumers in a timely manner.

2. In November 2016, Aptos discovered a data breach involving the theft of customers' personal information with an unknown number of compromised customer accounts (the "Security Breach"). After removing the malicious software causing the Security Breach in December 2016, Aptos waited two months to disclose the Security Breach to its clients, including Tempur Sealy, until February 5, 2017.

3. Upon learning of the Security Breach on or about February 5, 2017, Tempur Sealy waited nearly two months before disclosing the breach to their customers on or about April 4, 2017.

4. According to Tempur Sealy, the following customer information was compromised in the Security Breach: name, address, email address, telephone number, payment card account number, and expiration date (the "Personal Information").

5. Defendants' security failures enabled intruders to intercept, access and acquire Personal Information from within Aptos' systems and, on information and belief, subsequently make unauthorized purchases on consumers' credit and debit cards, while otherwise putting Class members' Personal Information at serious and ongoing risk. The intruders continue to use the Personal Information they obtained

as a result of Defendants' inadequate security to exploit consumers and Class members throughout the country.

6. The Security Breach was caused and enabled by Defendants' knowing violation of its obligations to abide by best practices and industry standards in protecting customers' Personal Information and/or its negligence in protecting Class members' Personal Information. Defendants' ongoing failure to maintain and comply with security standards between February and December 2016 allowed their customers' Personal Information to be compromised.

7. Defendants also failed to disclose the extent of the Security Breach and notify their affected customers in a timely manner. Defendants failed to take other reasonable steps to clearly and conspicuously inform their customers of the nature and extent of the Security Breach. By failing to provide adequate notice, Defendants prevented Class members from protecting themselves from the Security Breach.

8. Plaintiff retains a significant interest in ensuring that her Personal Information is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and similarly situated consumers whose Personal Information was stolen as a result of the Security Breach. Plaintiff asserts claims against Defendants for violations of state consumer protection statutes, state data

breach statutes, negligence, breach of implied contract and unjust enrichment. Plaintiff, on behalf of herself and similarly situated consumers, seeks to recover damages, including actual and statutory damages, and equitable relief, including injunctive relief to prevent a recurrence of the data breach and resulting injury, restitution, disgorgement and reasonable costs and attorneys' fees.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this Class action pursuant to 28 U.S.C. § 1332(d)(2). The claims of the Class members are in excess of $5,000,000 in the aggregate, exclusive of interest and costs, and at least one member of the Class is a citizen of a state different from at least one of the Defendants. For example, Plaintiff is a citizen of New York and Defendant Aptos is a citizen of Georgia.

10. This Court has jurisdiction over Defendants because they transact business in this state, have purposely availed themselves of the laws of this state, and because a substantial part of the events giving rise to Plaintiff's causes of action occurred in this state. In addition, Defendant Aptos resides in this District. Therefore venue is appropriate pursuant to 28 U.S.C. § 1391.

PARTIES

11. Plaintiff realleges, as if fully set forth, each and every allegation herein.

12. Plaintiff, Michelle Provost, is a resident of Rockland County, New York. Plaintiff used her debit card to make two online purchases from Tempur Sealy on April 11, 2016 and June 16, 2016. Plaintiff first learned of the fact that her debit card information was compromised when she received a written notification from Tempur Sealy in or about early April, 2017. Upon reviewing her bank statement(s) after receipt of the notice, she identified at least one charge, made on April 22, 2016 which, upon information and belief, involved a fraudulent charge

13. Plaintiff would not have used her debit card to make purchases from Tempur Sealy's online store had Defendants told her that Aptos lacked adequate computer systems and data security practices to safeguard customers' Personal Information from theft.

14. Plaintiff suffered actual injury from having her debit card account and Personal Information compromised and stolen in and as a result of the Security Breach.

15. Plaintiff suffered actual injury and damages by paying money to and purchasing products from Tempur Sealy during the Security Breach that she would not have paid had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' Personal Information and had Defendants provided timely and accurate notice of the data breach.

16. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her personal and financial identity information—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of purchasing Tempur Sealy's products and which was compromised in and as a result of the Security Breach.

17. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her Personal Information being placed in the hands of criminals who have already misused such information stolen in the Security Breach via sale of Plaintiff's and Class members' Personal Information on the Internet black market. Plaintiff has a continuing interest in ensuring that her Personal Information, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

18. Plaintiff was not reimbursed for any fraudulent charge(s) on her account.

19. Defendant Aptos, Inc. is a corporation based in Atlanta, Georgia.

20. Defendant Tempur Sealy International, Inc. is a Delaware corporation based in Lexington, Kentucky.

STATEMENT OF FACTS

21. Defendant Aptos owns and operates an online platform that provides retail enterprise management solutions. The company, through its platform, offers point of sale, digital commerce, order management, merchandising, analytics, and customer relationship management solutions to online retailers, like Tempur Sealy.

22. Defendant Tempur Sealy operates the website Tempurpedic.com through which it sells mattresses, pillows, and bedding. Like many other retail businesses, Tempurpedic.com accepts debit and credit card payments. Until October 2016, Tempur Sealy's website and online payment system was hosted and maintained by Aptos.

23. In February 2016, an unauthorized individual electronically accessed and instructed malware designed to capture historical payment card information provided to Aptos on Aptos' platform holding Information for 40 online retailers, including Tempur Sealy.[1]

[1] Neither Aptos nor Tempur Sealy have disclosed the extent of the Security Breach including, how many consumers' Personal Information was compromised and/or the time frame of the stolen records.

24. Aptos discovered the Security Breach in November 2016.[2]

25. In December 2016, Aptos contacted Federal law enforcement agencies and the U.S. Department of Justice to report the breach. Law enforcement requested that notification to businesses (including Tempur Sealy) be delayed to allow the investigation to move forward.

26. On or about February 6, 2017, Aptos began notifying its business clients of the Security Breach.

27. Aptos took no steps to inform consumers about the Security Breach. Instead, Aptos let the online businesses effected decide if, how, and when to notify their customers. Aptos refused to provide a list of businesses affected by the Security Breach.

28. On or about April 4, 2017, almost two (2) months after it received notice of the Security Breach from Aptos, Tempur Sealy notified its customers that their Personal Information provided in connection with purchases made prior to October 2016[3] may have been compromised.

---

[2] See Liberty Hardware, Notice of Data Breach (February 2017), https://dojmt.gov/wp-content/uploads/Liberty-Hardware-Manufacturing-Corporation.pdf ((last visited May 9, 2017).

[3] According to Tempur Sealy, "the Tempur-Pedic website was transitioned to a new hosting vendor in October of 2016, so this incident does not affect any customers who have made purchases on the website after September 30, 2016."

29. According to Tempur Sealy, the following Personal Information was compromised in the Security Breach: name, address, email address, telephone number, payment card account number, and expiration date.

30. Defendant's failure to adequately secure and protect consumers' Personal Information has placed Class members at increased risk of harm from the theft of their Personal Information.

31. Defendant's failure to disclose the Security Breach in a timely manner has placed Class members at increased risk of harm from the theft of their Personal Information.

32. Defendants allowed widespread and systematic theft of their customers' Personal Information. Defendants' actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' Personal Information.

Security Breaches Lead to Identity Theft

33. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[4] As the GAO Report states, this type of

[4] *See* http://www.gao.gov/new.items/d07737.pdf (last visited May 9, 2017).

identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely affect the victim's credit rating. In addition, the GAO Report states that victims of identity theft "face substantial costs and time to repair the damage to their good name and credit record."[5]

34. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumer's finances, credit history and reputation and can take time, money and patience to resolve.[6] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[7]

35. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [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

---

[5] *Id*. at 2.

[6] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2013), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited May 9, 2017).

[7] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

> 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.

36. According to the FTC, quick notification to persons whose personal information has been compromised allows them to take steps to limit the damage done by the breach, which may reduce the chance that the information will be misused.[8]

Personal Identity and Financial Information is Valuable Property

37. At a FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[9]

---

[8] *Data Breach Response: A Guide for Business*, https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business (last visited May 9, 2017).

[9] *The Information Marketplace: Merging and Exchanging Consumer Data*, https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited May 9, 2017).

38. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[10]

39. The FTC has also recognized that consumers' data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[11]

40. Recognizing the high value that consumers place on their personal information, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent,

---

[10] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited December 16, 2015).

[11] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited May 9, 2017).

consumers will make a profit from the surrender of their personal information.[12] This business has created a new market for the sale and purchase of this valuable data.[13]

41. Consumers place a high value not only on their personal information, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[14]

42. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website.[15]

---

[12] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited May 9, 2017).

[13] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited May 9, 2017).

[14] Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011), pre-publication version available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf (last visited May 9, 2017).

[15] Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, available at

43. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' personal information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

44. In addition, members of the payment card industry ("PCI") established a Security Standards Counsel ("PCI SSC") in 2006 to develop PCI Data Security Standards ("PCI DSS") for increased security of payment processing systems.

45. The PCI DSS provides, "PCI DSS applies to all entities involved in payment card processing – including merchants."[16]

46. Furthermore, according to the PCI DSS, "A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf," however, this does not absolve them of their duty ensure proper data security standards. According to the PCI DSS, "merchants and

---

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.200.6483&rep=rep1&type=pdf (emphasis added) (last visited May 9, 2017).

[16] *Requirements and Security Assessment Procedures, Version 3.2*, Payment Card Industry Data Security Standard, at 5 (April 2016), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf. (last visited May 9, 2017).

service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data."[17]

47. Tempur Sealy is a merchant that accepts payment cards through their Third Party Service Provider, Aptos.

48. The PCI DSS requires merchants and service providers to, among other things, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, and regularly monitor and test networks.

49. On information and belief, Defendants failed to comply with the PCI DSS, resulting in the Security Breach.

50. Tempur Sealy's Privacy Policy, as of its last update in February 2016, states "We seek to keep your Personal Information secure and implement reasonable technical, administrative and physical safeguards to help us protect such information from unauthorized access, use and disclosure." Tempur Sealy also states that in the event any Personal Information is compromised as a result of a breach of security, Tempur Sealy will take reasonable steps to investigate and notify individuals whose information is compromised and take other action in accordance with any applicable laws and regulations.

---

17 *Id.* at 12.

Damages Sustained By Plaintiff and the Class

51. A portion of the goods and services purchased from Tempur Sealy by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of personal information, including their credit and debit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the products purchased from Tempur Sealy.

52. Members of the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals and/or related bank fees charged to their accounts.

53. Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Defendants' wrongful conduct.

54. Moreover, as explained above, fraudulent use of cards might not be apparent for years. Therefore, consumers must expend considerable time taking these precautions for years to come.

55. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to

expend to monitor their financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

CLASS ALLEGATIONS

56. Pursuant to Fed. R. Civ. P. 23, Plaintiff asserts her claims that Defendants violated state consumer statues (Count I) and state data breach notification statutes (Count II) on behalf of separate statewide classes defined as follows:

> **Statewide [Consumer Protection or Data Breach Notification] Classes:**
>
> All residents of New York State whose Personal Information was compromised as a result of the data breach first disclosed by Tempur Sealy in April 2017.

57. Plaintiff asserts the state consumer law claims (Count I) under the listed consumer protection laws of Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South

Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wyoming, and the District of Columbia.

58. Plaintiff asserts the state data breach notification law claims (Count II) on behalf of separate statewide classes in and under the respective data breach statutes of the States of Alaska, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia..

59. Pursuant to Fed. R. Civ. P. 23, Plaintiff asserts her common law claims for negligence (Count III), breach of implied contract (Count IV), and unjust enrichment (Count V) on behalf of a nationwide class, defined as follows:

Nationwide Class:

All residents of the United States whose Personal Information was compromised as a result of the data breach first disclosed by Tempur Sealy in April 2017.

60. Defendants' conduct resulted in the Security Breach, which took place exclusively, or primarily, in Georgia. Accordingly, this Court has general

jurisdiction over Defendants and original jurisdiction over Plaintiff's claims. Applying Georgia law, therefore, comports with due process.

61. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims for negligence (Count III), breach of implied contract (Count IV), and unjust enrichment (Count V) under the laws of the individual States and Territories of the United States, and on behalf of separate statewide classes, defined as follows:

> **Statewide [Negligence, Breach of Implied Contract, or Unjust Enrichment] Classes:**
>
> All residents of New York State whose Personal Information was compromised as a result of the data breach first disclosed by Tempur Sealy in April 2017.

62. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which Defendants have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

63. Each of the proposed classes meet the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3):

64. **Numerosity**. The proposed classes include many thousands of customers whose data was compromised in the Security Breach. While the precise number of Class members in each proposed class has not yet been determined, the massive size of the Security Breach indicates that joinder of each member would be impracticable.

65. **Commonality**. Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. whether Defendants engaged in the conduct alleged herein;

b. whether Defendants' conduct constituted Deceptive Trade Practices (as defined below) actionable under the applicable consumer protection laws;

c. whether Defendants had a legal duty to adequately protect Plaintiff's and Class members' Personal Information;

d. whether Defendants breached their legal duty by failing to adequately protect Plaintiff's and Class members' Personal Information;

e. whether Defendants had a legal duty to provide timely and accurate notice of the Security Breach to Plaintiff and Class members;

f. whether Defendants breached their duty to provide timely and accurate notice of the Security Breach to Plaintiff and Class members;

g. whether and when Defendants knew or should have known that Aptos' computer systems were vulnerable to attack;

h. whether Plaintiff and Class members are entitled to recover actual damages and/or statutory damages; and

i. whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

66. **Typicality**. Plaintiff's claims are typical of the claims of the Class. Plaintiff and Class members were injured through Defendants' uniform misconduct and their legal claims arise from the same core Defendants practices.

67. **Adequacy**. Plaintiff is an adequate representative of the proposed classes because her interests do not conflict with the interests of the Class members

she seeks to represent. Plaintiff's counsel are very experienced in litigating consumer class actions and complex commercial disputes.

68. **Superiority**. A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendants. Even if it were economically feasible, requiring thousands of injured Plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

69. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted or have refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

70. Finally, all members of the purposed Classes are readily ascertainable. Defendants have access to addresses and other contact information for thousands of members of the Classes, which can be used to identify Class members.

COUNT I
VIOLATIONS OF STATE CONSUMER LAWS

(ON BEHALF OF PLAINTIFF AND THE SEPARATE STATEWIDE CONSUMER LAW CLASSES)

71. Plaintiff realleges, as if fully set forth, each and every allegation herein.

72. Plaintiff and members of the statewide Consumer Law Classes (the "Class" for purposes of this claim) are consumers who used their credit or debit cards to purchase products from Tempur Sealy primarily for personal, family, or household purposes.

73. Tempur Sealy, through Aptos, engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods and services to consumers, including Plaintiff and members of the Class.

74. Tempur Sealy, through Aptos, is engaged in, and its acts and omissions affect, trade and commerce. Defendants' acts, practices, and omissions were done in the course of Tempur Sealy's business of marketing, offering for sale, and selling goods and services throughout the United States and in each State and the District of Columbia through a website maintained and hosted by Aptos.

75. Defendants' conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices (collectively, "Deceptive Trade Practices"), including, among other things, Defendants':

a. failure to maintain adequate computer systems and data security practices to safeguard customers' Personal Information;

b. failure to disclose that their computer systems and data security practices were inadequate to safeguard customers' Personal Information from theft; and

c. failure to timely and accurately disclose the data breach to Plaintiff and Class members.

76. By engaging in such Deceptive Trade Practices, Defendants' have violated state consumer laws, including those that prohibit:

a. representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

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

c. omitting material facts regarding the goods and services sold;

d. engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;

e. unfair methods of competition;

f. unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices; and/or

g. similar prohibitions under the state consumer laws identified below.

77. As a direct result of Defendants 's violating state consumer laws, Plaintiff and Class members suffered damages that include:

a. fraudulent charges on their debit and credit card accounts, some of which were never reimbursed;

b. theft of their Personal Information by criminals;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with the fraudulent use of their financial accounts;

e. loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

f. costs and lost time associated with handling the administrative consequences of the Security Breach, including identifying, disputing, and seeking reimbursement for fraudulent charges,

cancelling and activating payment cards, and shopping for credit monitoring and identity theft protection;

g. purchasing products from Tempur Sealy that they would not have purchased, or would have not had paid the same price for, had they known of Defendants' Deceptive Trade Practices; and

h. impairment to their credit scores and ability to borrow and/or obtain credit.

78. Defendants' Deceptive Trade Practices violate the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-5(2), (3), (5), (7), and (27), *et seq*.;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq*.;

d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. & Prof. Code, § 17200, *et seq*.

e. The Colorado Consumer Protection Act, Colo. Rev. Stat. §§ 6-1-105(1)(b), (c), (e) and (g), *et seq*.;

f. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq*.;

g. The Delaware Consumer Fraud Act, Del. Code Ann. tit. 6 § 2513, *et seq*.;

h. The District of Columbia Consumer Protection Act, D.C. Code Ann. §§ 28-3904(a), (d), (e), (f) and (r), *et seq*.;

i. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. ch. 501.204(1), *et seq*.;

j. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (3), (5), and (7), *et seq*.;

k. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq*.; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq*.;

l. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq*.; and Idaho Code § 48-603C, *et seq*.;

m. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq*., and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Stat. § 510/2(a)(5), (7) and (12), *et seq*.;

n. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq*.;

o. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq*. (Plaintiff have obtained the approval of the Iowa Attorney General for filing this class action lawsuit as provided under I.C.A § 714H.7);

p. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq*.;

q. The Kentucky Consumer Protection Act, Ky. Rev. Stat. §§ 367.170(1) and (2), *et seq*.;

r. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq*.;

s. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), *et seq*., and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq*.;

t. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), (ii) and (iv), (5)(i), and (9)(i), *et seq*.;

u. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq*.;

v. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c),(e), (s) and (cc), *et seq*.;

w. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), *et seq*., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

x. The Mississippi Consumer Protect Act, Miss. Code Ann. §§ 75-24-5(1), (2)(b), (c), (e), and (g), *et seq*.;

y. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq*.;

z. The Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-103, *et seq*.;

aa. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq*.;

bb. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq*.;

cc. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq*.;

dd. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq*.;

ee. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq*.;

ff. The New York Business Law, N.Y. Gen. Bus. Law § 349(a);

gg. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq*.;

hh. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq*.;

ii. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq*.

jj. The Oklahoma Consumer Protection Act, 15 Okla. Stat. Ann. § 753(5), (7) and (20), *et seq*.;

kk. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e), (g) and (u), *et seq*.;

ll. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq*.;

mm. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq*.;

nn. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq*.;

oo. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq*.;

pp. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a), (b)(2), (3), (5), and (7), *et seq*.;

qq. The Texas Deceptive Trade Practices - Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq*.;

rr. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1), (2)(a), (b), and (i), *et seq*.;

ss. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq*.;

tt. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5), (6) and (14), *et seq*.;

uu. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq*.;

vv. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.; and

ww. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq*. and § 40-12-108.

79. Because of Defendants' Deceptive Trade Practices, Plaintiff and the Class members are entitled to relief, including restitution of the costs associated with the data breach, disgorgement of all profits accruing to Defendants because of its Deceptive Trade Practices, attorneys' fees and costs, and a permanent injunction enjoining Defendants from their Deceptive Trade Practices.

80. Plaintiff brings this claim on behalf of herself and the Class members for the relief requested and to benefit the public interest. This claim supports the public interests in assuring that consumers are provided truthful, non-deceptive information about potential purchases and protecting members of the public from Defendants' Deceptive Trade Practices. Defendants' wrongful conduct, including its Deceptive Trade Practices, has affected the public at large because a large number of individuals residing in the U.S. have been affected by Defendants' conduct.

COUNT II
VIOLATIONS OF STATE DATA BREACH NOTIFICATION STATUTES
(ON BEHALF OF PLAINTIFF AND THE SEPARATE STATEWIDE DATA BREACH STATUTE CLASSES)

81. Plaintiff realleges, as if fully set forth, each and every allegation herein.

82. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally apply to any person or business conducting business within the state that owns or licenses computerized data containing personal information. If the personal information is acquired or accessed in a way that compromises its security or confidentiality, the covered entity must notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

83. The Security Breach constituted a security breach that triggered the notice provisions of the data breach statutes and the Personal Information taken includes categories of personal information protected by the data breach statutes.

84. Defendants unreasonably delayed in informing Plaintiff and members of the statewide Data Breach Statute Classes ("Class," as used in this Claim II), about the data breach after Defendants knew or should have known that the data breach had occurred.

85. Plaintiff and Class members were damaged by Defendants' failure to comply with the data breach statutes.

86. Had Defendants' provided timely and accurate notice, Plaintiff and Class members could have avoided or mitigated the harm caused by the data breach. For example, they could have contacted their banks to cancel any affected cards before fraudulent charges were made, taken security precautions in time to prevent or minimize identity theft, or could have avoided using compromised payment cards during subsequent purchases.

87. Defendants' failure to provide timely and accurate notice of the Security Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), et seq.;

b. Ark. Code Ann. § 4-110-105(a), et seq.;

c. Cal. Civ. Code § 1798.83(a), et seq.;

d. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;

f. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;

g. D.C. Code § 28-3852(a), et seq.;

h. Fla. Stat. Ann. § 501.171(4), et seq.;

i. Ga. Code Ann. § 10-1-912(a), et seq.;

j. Haw. Rev. Stat. § 487N-2(a), et seq.;

k. Idaho Code Ann. § 28-51-105(1), et seq.;

l. Ill. Comp. Stat. Ann. 530/10(a), et seq.;

m. Iowa Code Ann. § 715C.2(1), et seq.;

n. Kan. Stat. Ann. § 50-7a02(a), et seq.;

o. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;

p. La. Rev. Stat. Ann. § 51:3074(A), et seq.;

q. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), et seq.;

s. Mich. Comp. Laws Ann. § 445.72(1), et seq.;

t. Minn. Stat. Ann. § 325E.61(1)(a), et seq.;

u. Mont. Code Ann. § 30-14-1704(1), et seq.;

v. Neb. Rev. Stat. Ann. § 87-803(1), et seq.;

w. Nev. Rev. Stat. Ann. § 603A.220(1), et seq.;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;

y. N.J. Stat. Ann. § 56:8-163(a), et seq.;

z. N.Y. Information Security Breach and Notification Act, § 899-aa of the N.Y. GBL;

aa. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;

bb. N.D. Cent. Code Ann. § 51-30-02, et seq.;

cc. Okla. Stat. Ann. Tit. 24 § 163(A), et seq.;

dd. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;

ee. R.I. Gen. Laws Ann. § 11-49.2-3(a), et seq.;

ff. S.C. Code Ann. § 39-1-90(A), et seq.;

gg. Tenn. Code Ann. § 47-18-2107(b), et seq.;

hh. Tex. Bus. & Com. Code Ann. § 521.053(b), et seq.;

ii. Utah Code Ann. § 13-44-202(1), et seq.;

jj. Va. Code. Ann. § 18.2-186.6(B), et seq.;

kk. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;

ll. Wis. Stat. Ann. § 134.98(2), et seq.; and

mm. Wyo. Stat. Ann. § 40-12-502(a), et seq.

88. Plaintiff and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to a) damages suffered by Plaintiff and Class members as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

COUNT III
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE STATEWIDE NEGLIGENCE CLASSES)

89. Plaintiff reallege, as if fully set forth, each and every allegation herein.

90. Defendants came into possession, custody, and/or control of personal and/or financial information of Plaintiff and Class members.

91. Defendants owed a duty to Plaintiff and to members of the Nationwide Class, or, alternatively, members of the separate Statewide Negligence Classes ("Class" as used in this Count III) to exercise reasonable care in safeguarding and securing the personal and/or financial information of Plaintiff and Class members in its possession, custody, and/or control.

92. Defendants had a duty to exercise reasonable care in implementing and maintaining reasonable procedures and practices appropriate for maintaining the safety and security of Plaintiff and Class members' personal and/or financial information in its possession, custody, and/or control.

93. Defendants had a duty to exercise reasonable care in timely notifying Plaintiff and Class members of an unauthorized disclosure of Plaintiff and Class members' personal and/or financial information in its possession, custody, and/or control.

94. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in safeguarding and securing the personal and/or financial information of Plaintiff and Class members in its possession, custody, and/or control.

95. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in implementing and maintaining reasonable procedures and practices appropriate for maintaining the safety and security of Plaintiff and Class members' personal and/or financial information in its possession, custody, and/or control.

96. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in timely notifying Plaintiff and Class members of an unauthorized disclosure of Plaintiff and Class members' personal and/or financial information in its possession, custody, and/or control.

97. Defendants' negligent and wrongful breach of duties owed to Plaintiff and Class members proximately caused an unauthorized disclosure of Plaintiff and

Class members' personal and/or financial information in its possession, custody, and/or control.

98. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE STATEWIDE BREACH OF IMPLIED CONTRACT CLASSES)

99. Plaintiff realleges, as if fully set forth, each and every allegation herein.

100. When Plaintiff and the members of the Nationwide class or, alternatively, the members of the separate Statewide Breach of Implied Contract Classes (collectively, the "Class" as used in this Count), provided their Personal Information to Defendants in making purchases from Tempur Sealy, they entered into implied contracts by which Defendants agreed to protect their Personal Information and timely notify them in the event of a data breach.

101. Defendants invited customers, including Plaintiff and Class members, to purchase products from Tempur Sealy using credit or debit cards in order to increase sales by making purchases more convenient. The Personal Information

also is valuable to Defendants, because Defendants use it for ancillary marketing and business purposes.

102. An implicit part of the offer was that Defendants would safeguard the Personal Information using reasonable or industry-standard means and would timely notify Plaintiff and the Class in the event of a data breach.

103. Based on the implicit understanding, Plaintiff and the Class accepted the offers and provided Defendants with their Personal Information by using their credit or debit cards in connection with purchases from Tempur Sealy during the period of the Security Breach.

104. Plaintiff and Class members would not have provided their Personal Information to Defendants had they known that Defendants would not safeguard their Personal Information as promised or provide timely notice of the Security Breach.

105. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants.

106. Defendants breached the implied contracts by failing to safeguard Plaintiff's and Class members' Personal Information and failing to provide them with timely and accurate notice when their Personal Information was compromised in the Security Breach.

107. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendants' breaches of the implied contracts with them.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE STATEWIDE UNJUST ENRICHMENT CLASSES)

108. Plaintiff realleges, as if fully set forth, each and every allegation herein.

109. Plaintiff and members of the Nationwide class or, alternatively, the members of the separate Statewide Unjust Enrichment Classes (collectively, the "Class" as used in this Count), conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Tempur Sealy at retail prices and provided Defendants with their Personal Information by using their credit or debit cards for the purchases. In exchange, Plaintiff and Class members should have been compensated by Defendants with the goods and services that were the subject of the transaction and by having Defendants process and store their Personal Information using adequate data security.

110. Defendants knew that Plaintiff and the Class conferred a benefit on Defendants. Defendants profited from their purchases and used their Personal Information for its own business purposes.

111. Defendants failed to secure the Plaintiff's and Class members' Personal Information, and, therefore, did not provide full compensation for the benefit the Plaintiff and Class members provided.

112. Defendants acquired the Personal Information through inequitable means because it failed to disclose the inadequate security practices previously alleged.

113. Had Plaintiff and Class members known that Defendants would not secure their Personal Information using adequate security, they would not have completed their purchases with Defendants.

114. Plaintiff and the Class have no adequate remedy at law.

115. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

116. Defendants should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiff and Class members proceeds that it

unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and the Class overpaid.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Classes set forth herein, respectfully request that the Court enter judgment in their favor that:

A. certifies the Classes requested, appoints the Plaintiff as class representative of the applicable classes and their undersigned counsel as Class counsel;

B. awards the Plaintiff and Class members appropriate monetary relief, including actual and statutory damages, restitution, and disgorgement;

C. on behalf of Plaintiff and the Statewide Classes, enters an injunction against Defendants 's Deceptive Trade Practices and requires Defendants to implement and maintain adequate security measures, including the measures specified above to ensure the protection of Plaintiff's Personal Information, which remains in the possession of Defendants ;

D. on behalf of Plaintiff and the Statewide Data Breach Statute Classes, awards appropriate equitable relief, including an injunction requiring Defendants to promptly notify all affected customers of future data breaches;

E. orders Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

F. awards Plaintiff and the Classes pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

G. awards such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all issues so triable.

June 9, 2017

Respectfully submitted,

/s/ David J. Worley
David J. Worley
Ga. Bar No. 776665
James M. Evangelista
Ga. Bar No. 707807
Kristi Stahnke McGregor
Ga. Bar No. 674012
EVANGELISTA WORLEY, LLC
8100A Roswell Road
Suite 100
Atlanta, GA 30350
Phone: (404)205-8400
Fax: (404)205-8395
jim@ewlawllc.com
david@ewlawllc.com
kristi@ewlawllc.com

William B. Federman (to be admitted *pro hac vice*)
Oklahoma Bar No. 9467

FEDERMAN & SHERWOOD
10205 N. Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
405.235.1560 (*telephone*)
405.239.2112 (*facsimile*)
wbf@federmanlaw.com
Gary S. Graifman, Esq.
Jay I. Brody, Esq.
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Road
Chestnut Ridge, New York 10977
(845) 356-2570 (*telephone)*
(845) 356-4335 *(facsimile)*
ggraifman@kgglaw.com
jbrody@kgglaw.com

Counsel to Plaintiff