UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

DARREN GLEAN and JAMES HUNTER, individually and on behalf of all others similarly situated,	§	
	§	CIVIL ACTION NO.:
Plaintiffs,	§	
	§	**CLASS ACTION COMPLAINT**
v.	§	
	§	**JURY TRIAL DEMANDED**
APTOS, INC., and TEMPUR SEALY INTERNATIONAL, INC.,	§	
Defendants.	§	

Plaintiffs, Darren Glean ("Mr. Glean" or "Glean") and James Hunter ("Mr. Hunter" or "Hunter") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, allege 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 themselves 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 Defendants' 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 "Aptos/TS Security Breach" or "Security Breach" hereinafter). 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 Aptos/TS 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 Aptos/TS 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 Aptos/TS 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 Aptos/TS Security Breach. By failing to provide adequate notice, Defendants prevented Class members from protecting themselves from the Aptos/TS Security Breach.

8. Plaintiffs retain a significant interest in ensuring that their Personal Information is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose

Personal Information was stolen as a result of the Aptos/TS Security Breach. Plaintiffs assert claims against Defendants for violations of state consumer protection statutes, state data breach statutes, negligence, breach of implied contract and unjust enrichment. Plaintiffs, on behalf of themselves and similarly situated consumers, seek 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 Hunter is a citizen of Washington 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 Plaintiffs' 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. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

12. Plaintiff Darren Glean, at all relevant times, has resided in Conyers, Georgia. In or about June, 2016, Mr. Glean purchased a mattress topper from Tempur Sealy on its e-commerce website, tempurpedic.com, using his Wells Fargo debit card. Unknown to Mr. Glean, his personal financial information was stolen in the data breach of the Tempur Sealy website, which website was managed and administered by Tempur Sealy and//or Aptos. This occurred despite the Aptos/Tempur Sealy Privacy Policy, a policy which Plaintiff read at the time of his purchase. In or about the spring of 2017, after receiving a notification from Tempur Sealy and/or Aptos about the data breach, Mr. Glean noticed numerous charges on his Wells Fargo debit card, the same card that he purchased the Tempurpedic mattress topper with. He discovered upon review, that certain charges were not made by him and, in fact, were made at store locations in states other than Georgia. Upon discovering those unauthorized and fraudulent charges, Mr. Glean complained to Wells Fargo and sought to have those unauthorized and

fraudulent charges reversed. Wells Fargo reversed certain charges but refused to reverse other unauthorized and fraudulent charges resulting in a loss to Mr. Glean of more than $300. As a result, Plaintiff canceled his Wells Fargo card and closed the account. Thereafter, he had to wait approximately one month to open a new account with Wells Fargo and get a new debit card for use. As a result, in addition to suffering financial injury, Mr. Glean was forced to spend time discussing the unauthorized and fraudulent charges with Wells Fargo personnel, and working with bank personnel to cancel ongoing charges. As a result, Mr. Glean suffered financial injury and loss of time and resources.

13. Plaintiff James Hunter, at all relevant times, is and was a resident of the State of Washington. On or about January 16, 2016, Mr. Hunter purchased 2 mattresses through a Mattress Firm outlet in Washington State and his order was submitted to Tempur Sealy's e-commerce website using his American Express credit card. Mr. Hunter, thereafter, was subjected to unauthorized and fraudulent charges charged to his credit card for approximately 6 months, in the sum of approximately $39 per month. Mr. Hunter discerned the charges were fraudulent and had the charges eventually cancelled. Mr. Hunter was forced to spend time travelling to his bank, reporting the unauthorized charges, and working with bank

personnel to cancel ongoing charges. As a result, Mr. Hunter suffered financial injury and loss of time and resources.

14. Plaintiffs would not have used their credit and/or debit cards to make purchases from or through Tempur Sealy's online store had Defendants told them that Aptos lacked adequate computer systems and data security practices to safeguard customers' Personal Information from theft.

15. Plaintiffs suffered actual injury and misuse from having their credit and/or debit card accounts and Personal Information compromised and stolen in the Aptos/TS Security Breach and as a result of said Security Breach.

16. In addition, Plaintiffs suffered actual injury and damages by paying money to and purchasing products from and/or through Tempur Sealy during the Aptos/TS Security Breach that they 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. In fact, Defendants claimed that online ecommerce purchases through their online site could be made safely and securely. In fact, Tempur Sealy and Aptos maintained online a "Privacy Policy" that stated, as of its last update in February 2016: "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 stated 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. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their personal and financial identity information—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Tempur Sealy's products and which was compromised in and as a result of the Aptos/TS Security Breach.

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

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. Aptos' own website discusses how it helps its clients mine the intrinsic value in their customers' data and Personal Information that Aptos collects for them. For example, under "Clienteling," Aptos touts the value of this information it harvests (https://www.aptos.com/solutions/crm-clienteling/clienteling/):

"Accessible knowledge:

> Aptos Clienteling puts detailed customer information at your fingertips. Sales associates can leverage historical customer data to

make compelling recommendations on new products and offers. They can easily see the "wardrobe view" of specific customers, understand their preferences, view their profiles and reference notes from previous visits.

Having this data at hand, your associates can focus on retention, reactivation, cross-selling and opportunity selling to keep your customers coming back more often, interest them in more items per visit and inspire them to spread the word. And when Clienteling is implemented with other Aptos solutions such as POS and Mobile POS, your customers' experiences—and your advantages—are further enriched."

24. Elsewhere on the site, Aptos explains:

Aptos CRM [Customer Relationship Management] combines activities from all channels into a single, cloud-based database that supports all users, retail structures, functions and brands, to give you a 360-degree view of each customer. A flexible retail data model and intuitive user interface lets authorized corporate employees or associates identify customers and look up their contact information, demographic profile, attributes and purchase history according to your rules. This ensures you can maximize CRM benefits and your control over how customer data is viewed and shared.

* * *

Whether your organization is new to customer relationship management or a sophisticated advocate, Aptos CRM has the resources you need to deliver and profitably apply meaningful insights from your customer data, to keep your customers engaged with your brand and motivated to buy. It's retail therapy that always pays off.

25. Indeed, if there was no ready market for personal and financial information, there would be no Aptos. Plaintiffs' personal information is valuable as it assists Defendants to develop sophisticated marketing programs.

26. 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]

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

28. 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.

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

---

[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.

[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).

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

31. On or about April 4, 2017, almost two (2) months after it received notice of the Aptos/TS 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.

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

33. 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.

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

[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."

35. 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

36. 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 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]

37. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumer's finances, credit history and reputation and can take

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

[5] *Id*. at 2.

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]

38. 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 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.

39. According to the FTC, quick notification to persons whose personal information has been compromised allows them to take steps to limit the damage

[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*.

done by the breach, which may reduce the chance that the information will be misused.[8]

Personal Identity and Financial Information is Valuable Property

40. 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]

41. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a

[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).

"new form of currency" that supports a $26 billion per year online advertising industry in the United States.[10]

42. 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]

43. If there is any doubt about the intrinsic value of individual consumers' personal information, one need only look at the explosion in sale of data in the area of micro-targeting such consumer information, which received recent in-depth discussion in the wake of Facebook's sale of such data for micro-targeting to Cambridge Analytica and the reaction thereto.

44. Recognizing the high value that consumers place on their personal information, many companies now offer consumers an opportunity to sell this

---

[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).

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, 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]

45. 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]

---

[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).

46. 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]

47. 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.

48. 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.

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

---

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

50. 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 to ensure proper data security standards. According to the PCI DSS, "merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data."[17]

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

52. 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.

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

54. 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

[17] *Id.* at 12.

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.

Damages Sustained By Plaintiffs and the Classes

55. Plaintiffs suffered actual injury and actual misuse of their credit and/or debit cards as a result of the Aptos/TS Security Breach.

56. In addition, Plaintiffs and Class members engaged in time and effort to remediate the effects of the breach and such time and effort is an element of Plaintiffs and the Classes' actual damages.

57. A portion of the goods and services purchased from and/or through Tempur Sealy by Plaintiffs and the Classes 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 Plaintiffs and the Classes were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the Classes incurred actual monetary damages in that they overpaid for the products purchased from Tempur Sealy.

58. Members of the Classes 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.

59. Plaintiffs and the Classes suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Defendants' wrongful conduct.

60. 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.

61. Plaintiffs and the Classes suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the Classes have been forced to expend to monitor their financial and bank accounts as a result of the Aptos/TS Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

CLASS ALLEGATIONS

62. Pursuant to Fed. R. Civ. P. 23, Plaintiff Glean asserts his claim that Defendants violated the Georgia Uniform Deceptive Trade Practices Act, Ga. Code Ann. §§ 10-1-370, *et seq*. (Count I), intends to assert, subject to the thirty (30) days from his May 3rd, 2018 demand passing in the event Defendants fail to agree to a

remedy for Plaintiff and the Georgia Class, a claim under the Georgia Fair Business Practices Act, Ga. Code Ann. § 10–1–390, *et seq*. (Count II), and asserts a claim that Defendants violated the Georgia data breach notification statutes (Count II) on behalf of himself and a Georgia statewide class defined as follows:

Georgia Class:

All residents of Georgia whose Personal Information was compromised as a result of the data breach first disclosed by Tempur Sealy in April 2017. ("Georgia Class")

63. Pursuant to Fed. R. Civ. P. 23, Plaintiff Hunter asserts his claims that Defendants violated Washington Consumer Protection Act, Wash. Rev. Code Ann. §§ 19.86.020, *et seq*. (Count IV) and Washington data breach notification statutes (Count V) on behalf of a Washington statewide class defined as follows:

Washington Class:

All residents of Washington whose Personal Information was compromised as a result of the data breach first disclosed by Tempur Sealy in April 2017. ("Washington Class")

64. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their common law claims for negligence (Count VI), breach of implied contract (Count VII), and unjust enrichment (Count VIII) 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.

65. 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 Plaintiffs' claims. Applying Georgia law, therefore, comports with due process.

66. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Glean asserts claims for negligence (Count VI), breach of implied contract (Count VII), and unjust enrichment (Count VIII) under the laws of the State of Georgia and on behalf of the Georgia Class.

67. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Hunter asserts claims for negligence (Count VI), breach of implied contract (Count VII), and unjust enrichment (Count VIII) under the laws of the State of Washington on behalf of the Washington Class.

68. 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.

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

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

71. **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 Plaintiffs' and Class members' Personal Information;

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

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

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

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

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

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

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

73. **Adequacy**. Plaintiffs are adequate representatives of the proposed classes because their interests do not conflict with the interests of the Class

members they seek to represent. Plaintiffs' counsel are experienced in litigating consumer class actions and complex commercial disputes.

74. **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.

75. 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.

76. 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
GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT
Ga. Code Ann. §§ 10-1-370, *et seq*.
(Asserted by Plaintiff Glean and the Georgia Class)

77. Plaintiff Glean ("Plaintiff" for purposes of this claim) realleges, as if fully set forth herein, each and every allegation previously set forth herein.

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

79. Defendants, Plaintiff, and Georgia Class Members are "persons" within the meaning of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), Ga. Code Ann. § 10-1-371(5).

80. The Georgia UDTPA prohibits "deceptive trade practices," which includes the misrepresentation of the standard, quality, grade or characteristics of goods or services, and engaging in "any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Ga. Code Ann. § 10-1-372(a).

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

82. 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, including Georgia, through a website maintained and hosted by Aptos.

83. 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;

c. failure to disclose and active concealment of its grave data-security defects as discussed herein,

d. employment of deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of material facts with intent that others rely upon such concealment,

suppression, or omission, in connection with accessing and storing the extremely sensitive and valuable Personal Information of Plaintiff and Class Members; and

e. failure to timely and accurately disclose the data breach to Plaintiffs and Class members.

84. By engaging in such Deceptive Trade Practices, Defendants' have violated the Georgia UDTPA, including the following prohibited conduct:

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; and/or

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

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

a. fraudulent charges on their debit and/or 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.

86. 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.

87. Plaintiff brings this claim on behalf of themselves and the Class members for the relief requested and to benefit the public interest. This claim supports the public interest 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., including in Georgia, have been affected by Defendants' conduct.

COUNT II
THE GEORGIA FAIR BUSINESS PRACTICES ACT
Ga. Code Ann. §§ 10-1-390, *et seq*.
(Asserted by Plaintiff Glean and the Georgia Class)

88. Plaintiff Glean ("Plaintiff" for purposes of this claim) realleges, as if fully set forth herein, each and every allegation set previously alleged herein.

89. The Georgia Fair Business Practices Act ("GFBPA") prohibits "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce," including, inter alia, "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another." Ga. Code Ann. § 10–1–393(a) and (b)(7).

90. By the acts and conduct alleged herein, Defendants committed unfair and deceptive acts and practices in the State of Georgia in violation of the GFBPA by making the misrepresentations and material omissions described above.

91. Defendants' unfair or deceptive acts and practices in connection with members of the Georgia Subclass, include, but are not limited to, the following:

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;

c. failure to disclose and active concealment of its grave data-security defects as discussed herein,

d. employment of deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of material

facts with intent that others rely upon such concealment, suppression, or omission, in connection with accessing and storing the extremely sensitive and valuable Personal Information of Plaintiff and Class Members; and

e. failure to timely and accurately disclose the data breach to Plaintiffs and Class members.

92. The foregoing acts, practices, and representations described in this section and those described throughout the Complaint amounted to a breach of a duty owed to the consuming public in general, as they were directed at consumers who might purchase Defendants' goods and/or services and impacted the consumer marketplace.

93. Defendants' unfair and deceptive acts and practices occurred in the conduct of trade and commerce, and has and continues to pose a risk to consumers and the consuming public generally. If not enjoined and addressed by the court, Defendants' unfair and deceptive practices are likely to be a recurring consumer threat to consumers purchasing their goods and/or services.

94. The foregoing deceptive acts and practices described in this section and throughout the Complaint were unfair and deceptive in a material way because they fundamentally misrepresented Defendant's goods and services, and caused Plaintiffs and members of the Georgia Subclass to reasonably believe that

Defendants' computer systems and data security practices were secure and adequate to safeguard their extremely sensitive and valuable Personal Information being accessed and stored by Defendants.

95. Plaintiff and members of the Georgia Class were injured as a direct and proximate result of Defendant's violation of the GFBPA which caused Class members the injury and/or damages described herein, including but not limited to:

a. fraudulent charges on their debit and/or 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.

96. Defendants knew or should have known that its computer systems and data security practices were not sufficiently secure and/or adequate to safeguard their extremely sensitive and valuable Personal Information being accessed and stored by Defendants. Defendants knew that its computer systems had security flaws which were inadequate to safeguard the Georgia Subclass Members' personal data and that the risk of a data breach or theft was high. Defendants' actions and violations of the law were negligent, knowing and willful, intentional, and/or wanton and reckless with respect to the rights of members of the Georgia Subclass.

97. Furthermore, pursuant to Ga. Code Ann. § 10-1-399(b), in a letter dated May 3, 2018 ("May 3rd Letter"), sent Certified Mail/Return Receipt Requested to Defendants, Plaintiff's counsel made a written demand for relief from

Defendants, on behalf of Plaintiff and others similarly situated who purchased Defendants' products and/or services through Tempur Sealy's e-commerce websites prior to or during the data breach which occurred on Defendants' websites. The letter identified the claimant and reasonably described the unfair or deceptive acts and practices relied upon and the injuries suffered. In the event Defendants fail to provide the relief requested in said letter within thirty (30) days, Plaintiff intends to amend and assert the claim in this Count as set forth below, which is included herein as a placeholder, for such claim in the event Defendant fails to provide said remedy.

98. By virtue of Defendant's misrepresentations and willful omissions, as well as their intentional violations of the GFBPA, Plaintiff and members of the Georgia Class have suffered damages. Accordingly, Plaintiff and the proposed Georgia Class, upon thirty (30) days passing without the remedy sought in the May 3rd Letter being agreed to, will seek to enjoin the unlawful acts and practices described herein; to recover actual damages; an award of treble damages; an award of punitive damages; and reasonable attorneys' fees and costs.

99. Because of Defendants' unfair and deceptive acts and practices, Plaintiff and the Class members would be 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.

100. Plaintiff intents to bring this claim on behalf of himself and the Class members for the relief requested and to benefit the public interest. This claim supports the public interest in assuring that consumers are provided truthful, non-deceptive information about potential purchases and protecting members of the public from Defendants' unfair and deceptive acts and 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., including in Georgia, have been affected by Defendants' conduct.

COUNT III
GEORGIA SECURITY BREACH NOTIFICATION ACT
Ga. Code Ann. §§ 10-1-912, *et seq*.
(Asserted by Plaintiff Glean and the Georgia Class)

101. Plaintiff Glean ("Plaintiff" for purposes of this claim) realleges, as if fully set forth herein, each and every allegation previously alleged herein.

102. Plaintiff asserts this claim on behalf of himself and members of the Georgia Class (the "Class" for purposes of this claim).

103. Defendants are required to accurately notify Plaintiff and Georgia Class Members if it becomes aware of a breach of their data security system (that

was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under Ga. Code Ann. § 10-1-912(a).

104. Defendants are businesses that own or license computerized data that includes personal information as defined by Ga. Code Ann. § 10-1-912(a).

105. Plaintiff and Georgia Class Members' Personal Information (e.g., Social Security numbers) includes personal information as covered under Ga. Code Ann. § 10-1-912(a).

106. The Security Breach constituted a security breach that triggered the notice provisions of Georgia Security Breach Notification Act and Washington Data Breach Notice Act and the Personal Information taken includes categories of personal information protected by the data breach statutes.

107. Because Defendants were aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Class Members' Personal Information), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

108. Defendants unreasonably delayed in informing Plaintiffs and members of the Georgia Class about the data breach after Defendants knew or should have known that the data breach had occurred.

109. Thus, by failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Ga. Code Ann. § 10-1-912(a).

110. As a direct and proximate result of Defendants' violations of Ga. Code Ann. § 10-1-912(a), Plaintiff and Georgia Class Members suffered damages, as described above.

111. Had Defendants' provided timely and accurate notice, Plaintiffs 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.

112. Plaintiffs and members of each of the Georgia Class seek all remedies available under Ga. Code Ann. § 10-1-912, including but not limited to a) damages suffered by Plaintiffs and Class members as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

COUNT IV
WASHINGTON CONSUMER PROTECTION ACT
Wash. Rev. Code Ann. §§ 19.86.020, et seq.
(Asserted by Plaintiff Hunter and the Washington Class)

113. Plaintiff Hunter ("Plaintiff" for purposes of this claim) realleges, as if fully set forth herein, each and every allegation previously alleged herein.

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

115. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce impacting consumers nationwide and in Washington, in violation of Wash. Rev. Code Ann. § 19.86.020, including but not limited to the following:

a. Misrepresenting and fraudulently advertising material facts pertaining to the sale of its goods and/or services to Washington Subclass Members by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Washington Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts pertaining to goods and/or services to the Washington Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Washington Class Members' Personal Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Washington Class Members' Personal Information;

d. Engaging in deceptive, unfair and unlawful trade acts or practices by failing to maintain the privacy and security of Washington Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach described herein. These unfair acts and practices violated duties imposed by laws and Washington regulations pertaining to Privacy of Consumer Financial and Health Information (Wash. ADC 284-04-300);

e. Failing to disclose Defendants' security breach to Washington Subclass Members in a timely and accurate manner, contrary to the duties imposed by Wash. Rev. Code Ann. § 19.255.010(1); and

f. Failing to take proper action following Defendants' security breach to enact adequate privacy and security measures and protect Washington Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

116. As a direct and proximate result of Equifax's deceptive trade practices, Washington Subclass Members suffered injury and/or damages.

117. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Washington Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

118. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard Washington Class Members' Personal Information and that risk of a data breach or theft was high. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Washington Class.

119. Plaintiff and Washington Class Members seek relief under Wash. Rev. Code Ann. § 19.86.090, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

COUNT V
WASHINGTON DATA BREACH NOTICE ACT
Wash. Rev. Code Ann. §§ 19.255.010, et seq.
(Asserted by Plaintiff Hunter and the Washington Class)

120. Plaintiff Hunter ("Plaintiff" for purposes of this claim) realleges, as if fully set forth herein, each and every allegation previously alleged herein.

121. Plaintiff asserts this claim on behalf of himself and members of the Washington Class (the "Class" for purposes of this claim).

122. Defendants are required to accurately notify Plaintiff and Washington Class Members following discovery or notification of the breach of their data security systems (if personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured) in the most expedient time possible and without unreasonable delay under Wash. Rev. Code Ann. § 19.255.010(1).

123. Defendants are businesses that own or license computerized data that includes personal information as defined by Wash. Rev. Code Ann. § 19.255.010(1).

124. Plaintiff's and Washington Class Members' Personal Information includes personal information as covered under Wash. Rev. Code Ann. § 19.255.010(5).

125. Because Defendants discovered a breach of its security system (in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1).

126. As a direct and proximate result of Defendants' violations of Wash. Rev. Code Ann. § 19.255.010(1), Plaintiff and Washington Class Members suffered damages, as described above.

127. Had Defendants' provided timely and accurate notice, Plaintiffs 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.

128. Plaintiff and Washington Class Members seek relief under Wash. Rev. Code Ann. §§ 19.255.010(10)(a) and 19.255.010(10)(b), including, but not limited to, actual damages and injunctive relief.

COUNT VI
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Separate Statewide Georgia and Washington Negligence Classes)

129. Plaintiffs reallege, as if fully set forth herein, each and every allegation previously alleged herein.

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

131. Defendants owed a duty to Plaintiffs 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 Plaintiffs and Class members in its possession, custody, and/or control.

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

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

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

135. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs 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 Plaintiffs and Class members' personal and/or financial information in its possession, custody, and/or control.

136. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to exercise reasonable care in timely notifying Plaintiffs and Class members of an

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

137. Defendants' negligent and wrongful breach of duties owed to Plaintiffs and Class members proximately caused an unauthorized disclosure of Plaintiffs and Class members' personal and/or financial information in its possession, custody, and/or control.

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

COUNT VII
BREACH OF IMPLIED CONTRACT IN FACT
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Separate Statewide Georgia and Washington Breach of Implied Contract Classes)

139. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

140. When Plaintiffs 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.

141. Defendants invited customers, including Plaintiffs 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.

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

143. Based on the implicit understanding, Plaintiffs 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.

144. Plaintiffs 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.

145. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants.

146. Defendants breached the implied contracts by failing to safeguard Plaintiffs' 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.

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

COUNT VII
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Separate Statewide Georgia and Washington Unjust Enrichment Classes)

148. Plaintiffs reallege, as if fully set forth herein, each and every allegation previously alleged herein.

149. Plaintiffs 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, Plaintiffs 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.

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

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

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

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

154. Plaintiffs and the Class have no adequate remedy at law.

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

156. Defendants should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class members proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and the Class overpaid.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, 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 Plaintiffs as class representatives of the applicable classes and their undersigned counsel as Class counsel;

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

C. on behalf of Plaintiffs 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 Plaintiffs 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 Plaintiffs 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

Plaintiffs demand a trial by jury on all issues so triable.

May 11, 2018

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 (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. (to be admitted *pro hac vice*)
Jay I. Brody, Esq. (to be admitted *pro hac vice*)
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Road
Chestnut Ridge, New York 10977
(845) 356-2570 (*telephone)*
ggraifman@kgglaw.com
jbrody@kgglaw.com

Counsel to Plaintiffs

JS44 (Rev. 6/2017 NDGA)

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

DARREN GLEAN and JAMES HUNTER, individually and on behalf of all others similarly situated,

DEFENDANT(S)

APTOS, INC., and TEMPUR SEALY INTERNATIONAL, INC.,

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Rockdale County, GA
(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

David J. Worley
EVANGELISTA WORLEY, LLC
8100A Roswell Road, Suite 100
Atlanta, GA 30350
Phone: (404)205-8400; david@ewlawllc.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION
(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ☐ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☑ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES
(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☑ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. ORIGIN (PLACE AN "X "IN ONE BOX ONLY)

- ☑ 1 ORIGINAL PROCEEDING
- ☐ 2 REMOVED FROM STATE COURT
- ☐ 3 REMANDED FROM APPELLATE COURT
- ☐ 4 REINSTATED OR REOPENED
- ☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Class Action pursuant to 28 U.S.C. § 1332(d)(2) whereby defendant, among other things, failed to adequately protect Plaintiffs' credit data in violation of statutory and common law.

(IF COMPLEX, CHECK REASON BELOW)

- ☐ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☑ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☐ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☐ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $**_____

JURY DEMAND ☑ **YES** ☐ **NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE Ross **DOCKET NO.** 1:17-CV-02120-ELR

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☑ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

- ☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

/s/ David J. Worley — May 11, 2017

SIGNATURE OF ATTORNEY OF RECORD **DATE**