Tammy Hussin (CA Bar No. 155290)
tammy@hussinlaw.com
HUSSIN LAW
1596 N. Coast Hwy 101
Encinitas, CA 92024
T: (877)677-5397
F: (877)667-1547

Gary E. Mason (DC Bar No. 418073)
gmason@masonllp.com
David K. Lietz (DC Bar No. 430557)
dlietz@masonllp.com
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
T: (202) 429-2290
F: (202) 429-2294

Gary M. Klinger (IL Bar No. 6303726)
gklinger@masonllp.com
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
T: (202) 429-2290
F: (202) 429-2294

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

APRIL FESLER, *individually and on behalf of all others similarly situated*,

Plaintiff,

v.

PETCO ANIMAL SUPPLIES STORES, INC and PUPBOX, INC.,

Defendants.

Case No. **'20CV2474 CAB LL**

CLASS ACTION

COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff April Fesler ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendants Petco Animal Supplies Stores, Inc. and PupBox, Inc. (collectively "Defendants"), to obtain damages, restitution, and injunctive relief for the Class, as defined below. Plaintiff makes the following allegations upon personal knowledge with respect to herself and on information and belief derived from, among other things, the investigation of counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyber-attack on Defendants' website that allowed an unauthorized third party to access Defendants' computer systems and data, resulting in the capture and removal of sensitive personal and financial information of over 30,000 customers from Defendants' website and network (the "Cyber-Attack").

2. As a result of the Cyber-Attack, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Plaintiff's and Class Members' sensitive personal and financial information—which was entrusted to Defendants—was compromised, unlawfully accessed, and stolen due to the Cyber-Attack. Information compromised and captured in the Cyber-Attack includes customers' names, email addresses, addresses, credit card numbers, credit card expiration dates, credit card CVV codes, and PupBox.com passwords; all of which Defendants collected and maintained (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated

to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

5. Defendants maintained the Private Information in a reckless manner.

6. In particular, the Private Information was collected and maintained on Defendants' website and computer network in a condition vulnerable to cyberattacks.

7. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to Defendants. Thus, Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left the property in a dangerous condition.

8. In addition, Defendants and their employees failed to properly monitor their website, computer network and systems that housed the Private Information.

9. Had Defendants properly monitored their property, they would have discovered the intrusion sooner.

10. What's more, Plaintiff's and Class Members' identities and financial security are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, *e.g.*, using Class Members' financial information to make unauthorized purchases and open various accounts.

12. As a further result of the Cyber-Attack, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against

fraud.

13. Plaintiff and Class Members have and may also incur out-of-pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect credit or payment card fraud.

14. For nearly six months, from February 11, 2020 until August 9, 2020, Private Information belonging to customers was captured by and shared with an unauthorized third-party.[1]

15. PupBox customers across the United States have suffered real and imminent harm as a direct consequence of Defendants' conduct, which includes (a) refusing to take adequate and reasonable measures to ensure its website and computer systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard customers' personal and financial information; and (d) failing to provide timely and adequate notice of the data breach.

16. As a result of the Cyber-Attack, the Private Information, which included but is not be limited to payment card data ("PCD") of approximately 30,000 PupBox customers, has been exposed to criminals for misuse.

17. The injuries suffered by Plaintiff and the proposed Classes as a direct result of the Cyber-Attack include, *inter alia*:

a. Unauthorized charges on their payment card accounts;

b. Theft of their personal and financial information;

c. Costs associated with the detection and prevention of unauthorized use of their financial accounts;

d. Loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in

[1] *See* https://oag.ca.gov/system/files/ExperianF8590L02PupBoxCA%20Template.docxSASPROOFRev1.pdf.

the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

f. The imminent and certainly impending injury flowing from potential fraud posed by their personal information and PCD being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class Members' information on the Internet black market;

g. Damages to and diminution in value of their personal and financial information entrusted to PupBox for the sole purpose of making purchases from PupBox and with the mutual understanding that PupBox would safeguard Plaintiff's and Class Members' data against theft and not allow access to and misuse of their information by others;

h. Money paid to PupBox during the period of the data breach in that Plaintiff and Class members would not have purchased from PupBox had Defendants disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Private Information and PCD and had PupBox provided timely and accurate notice of the data breach;

i. Continued risk to their personal information and PCD, which remains in the possession of PupBox and which is subject to further breaches so long as PupBox continues to fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data in its possession.

18. Examples of the harms to PupBox customers as a direct and foreseeable consequence of its conduct include the experience of the representative Plaintiff, which is described below.

19. Per the Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was captured and shared with an unauthorized third-party during the timeframe of the Data Breach.

20. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' website and data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

21. Accordingly, Plaintiff brings this action against Defendants seeking redress for its unlawful conduct asserting claims for negligence, negligence *per se*, violation of the Washington State Consumer Protection Act, violation of California's Unfair Competition Law and Consumer Records Act, breach of an implied contract, and unjust enrichment.

PARTIES

22. Plaintiff April Fesler is a resident of Aberdeen, Washington. She is (and was during the period of the Cyber-Attack) a citizen of the State of Washington.

23. Defendant Petco Animal Supplies Stores, Inc. ("Petco") is a Delaware corporation with its principal place of business at 10850 Via Frontera, San Diego, California 92127. Petco markets, advertises, distributes, and sells its products and services throughout the United States. In 2020, Petco reported revenue totaling $4.1

billion the previous year.[2]

24. Defendant PupBox, Inc. ("PupBox") is a California corporation with its principal place of business at 4060 Terrace Court, San Diego, California 92116. PupBox markets, advertises, distributes, and sells its products throughout the United States. In November 2017, PupBox was acquired by Petco Animal Supplies, Inc. and became a wholly owned subsidiary.[3]

25. Per the Notice Letter sent out on October 2, 2020, PupBox is an integrated business unit of Petco. Petco controls PupBox with the purpose of carrying out its business and operations from its headquarters in this District. On information and belief, Petco maintained the Private Information of Plaintiff and Class Members that they provided to PupBox in the course of transacting with PupBox. On information and belief, Petco maintained the Private Information of Plaintiff and Class Members in this District.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and one Defendant are citizens of different states. There are more than 30,000 putative Class Members.

27. This Court has personal jurisdiction over Defendants because its principal place of business is in California and has sufficient contacts in this District.

28. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendants conduct substantial business in this District and California is the principal place of business for Defendants.

---

[2] *See Petco Animal Supplies*, Forbes (last visited Dec. 10, 2020), https://www.forbes.com /companies/petco-animal-supplies/?sh=1dfe82627f78.

[3] *See* Jennifer Van Grove, *Petco Just Bought This San Diego Company You Saw on 'Shark Tank'*, The San Diego Union-Tribune (Nov. 15, 2017), https://www.sandiegouniontribune.com/business/technology/sd-fi-petco-pupbox-20171115-story.html.

STATEMENT OF FACTS

29. PupBox sells a monthly service to customers where it sends each customer a box containing dog treats, toys, and accessories each month. The company is based in San Diego, CA, USA, and according to SimilarWeb, the company averages approximately 319,000 website visitors each month.[4]

30. In a Notice of Data Breach sent to customers, the company explains that on August 7, 2020, "we received notification that fraudulent activities may have occurred on credit cards that were used on the PupBox website[.]"

> **What Happened**
>
> We are writing to inform you that on September 2, 2020, PupBox (a business unit of Petco Animal Supplies Stores, Inc.) became aware of a security incident which affected the PupBox website and may have resulted in a breach of your personal information. On August 7, 2020, we received a notification that fraudulent activities may have occurred on credit cards that were used on the PupBox website between February 26, 2020 and July 21, 2020. We promptly launched an investigation with the assistance of a leading cybersecurity firm, which revealed an unauthorized plugin on the PupBox website. The plugin allowed personal information to be captured and shared with a third-party server between February 11, 2020 and August 9, 2020.
>
> **What Information Was Involved?**
>
> The personal information exposed in this incident may include your name, email address, address, credit card number, credit card expiration date, credit card CVV code, and your Pupbox.com password. The investigation confirmed that there was no further sensitive information involved in this incident, such as Social Security Number.

31. PupBox commissioned an investigation into the incident and the investigation revealed " . . . an unauthorized plugin on the PupBox website. The plugin allowed personal information to be captured and shared with a third party server between February 11, 2020 and August 9, 2020."

32. This means that any customer who purchased from the website between February 2020 and August 2020 most likely had their personal and credit card

[4] *See Traffic Overview*, SimilarWeb (Dec. 14, 2020), https://www.similarweb.com/website/pupbox.com/#overview

information stolen. Stolen information included customers' names, email addresses, addresses, credit card numbers, credit card expiration dates, credit card CVV codes, and PupBox.com passwords.

33. Though PupBox claims to have shut down impacted systems when it found out about the unauthorized plugin on August 7, 2020. PupBox also states that customers personal information was being collected by the unauthorized third party until August 9, 2020.

34. In a series of notification letters to various states' Attorney Generals, PupBox states that they are notifying approximately 30,673 individuals.[5]

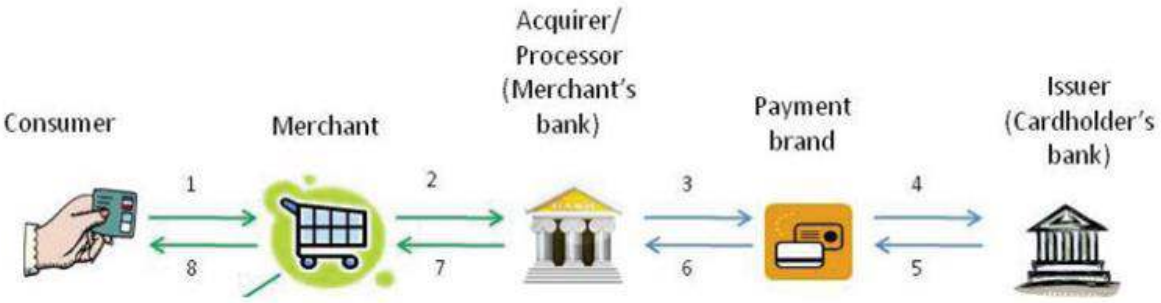
35. Defendants also substantially delayed providing notice of this Cyber-Attack. Despite finding out about the Cyber-Attack in early-August 2020, notice was not sent to PupBox customers until October 2, 2020, a delay of two months.

36. The Plaintiff in this case has already experienced substantial identity theft and financial fraud due to Defendants' failure to implement basic security measures.

37. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website) to pay for merchandise. The card is then "swiped" and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (*i.e.*, the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (*i.e.*, cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. See graphic below:[6]

[5] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a62632d4-568d-4100-85df-0b78ea165a25.shtml.

[6] Source: "Payments 101: Credit and Debit Card Payments," a white paper by First Data, at: https://www.firstdata.com/downloads/thought-leadership/payments101wp.pdf.



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

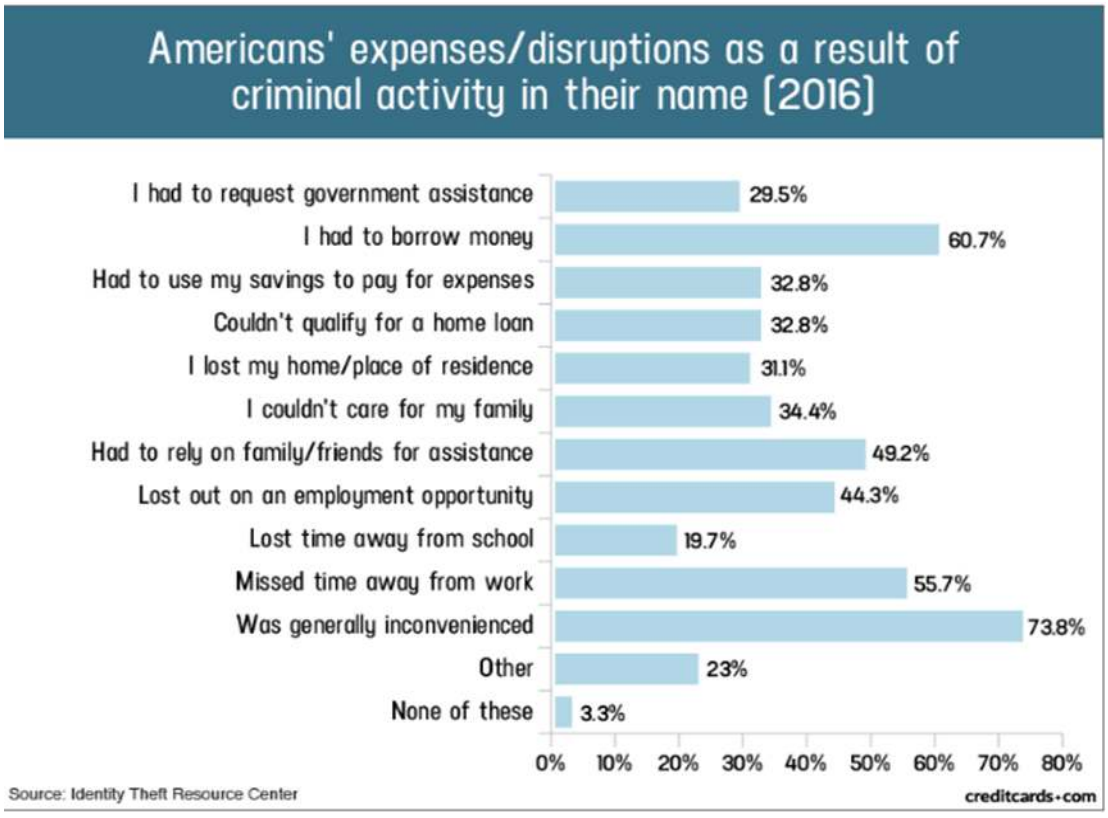
38. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

39. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment it is "swiped," hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the

cardholder's personal information stored in the retailer's computers.

40. On information and belief, the financial fraud suffered by Plaintiff and other customers demonstrate that Defendants chose not to invest in the technology to encrypt payment card data (PCD) at point-of-sale to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control employee credentials and access to computer systems to prevent a security breach and/or theft of PCD.

41. A 2016 study by the Identity Theft Resource Center (ITRC) shows the multitude of harms caused by fraudulent use of personal information:[7]



42. According to a 2018 survey conducted by ITRC, identity and financial fraud

[7] Robert Siciliano, et al., *Identity Theft: The Aftermath 2016*, Identity Theft Resource Center, https://www.idtheftcenter.org/images/page-docs/AftermathFinal2016.pdf (last visited Dec. 16, 2020).

results in significant emotional damage—over 83% of victims felt violated, angry, worried, and frustrated; 69.4% stated "they could not trust other and felt unsafe[;]" 67.3% reported feeling a sense of helplessness; and 59.2% of victims felt depressed.[8]

43. Plaintiff and the Class have experienced one or more of these harms as a result of the Cyber-Attack.

44. What's more, theft of Private Information is also gravely serious. PII is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

45. Also, there may be a time lag between when harm occurs versus when it is discovered, and also between when personal information or PCD is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[9]

46. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

47. There is a strong probability that entire batches of stolen information have

---

[8] *See* Jason Steele, *Credit Card Fraud and ID Theft Statistics*, CreditCards.com (Oct 23, 2020), https://www.creditcards.com/credit-ca rd-news/credit-card-security-id-theft-fraud-statistics1276.php (last visited Dec. 16, 2020).

[9] "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" by GAO, June 2007, at: https://www.gao.gov/assets/270/262904.html.

been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

48. Plaintiff and Members of the Classes defined below have or will suffer actual injury as a direct result of Defendants' data breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

49. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

50. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

51. As a direct and proximate result of the Data Breach, Plaintiff's PII and payment card data was exfiltrated and is in the hands of identity thieves and criminals,

as evidenced by the identity theft and fraud perpetrated against Plaintiff described above.

52. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered actual identity theft and fraud.

53. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff now has to take the time and effort to mitigate the actual and potential impact of the data breach on her everyday life, including placing "freezes" and "alerts" with credit reporting agencies, contacting his financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

54. Moreover, Plaintiff and the Class have an interest in ensuring that their information, which remains in the possession of Defendants is protected from further breaches by the implementation of security measures and safeguards.

55. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

56. Since the breach occurred, Plaintiff has received approximately 10–20 scam calls, which appeared to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

57. As a result of the Data Breach, Plaintiff has also received bank notices indicating fraudulent and unauthorized charges on her accounts.

58. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

59. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

60. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiff and Defendants included Defendants' contractual obligation to provide adequate data security, which Defendants failed to provide. Thus, Plaintiff and the Class Members did not get what they paid for.

61. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

62. Since the Data Breach, Plaintiff has spent a significant amount of time monitoring her credit via Experian and TransUnion, and has put a freeze on her credit.

63. Plaintiff has also spent time filing reports with the Federal Trade Commission and has attempted to implement a recover plan.

64. Plaintiff and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including personal information and PCD;

b. Improper disclosure of their personal information and PCD property;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers' personal information and PCD being placed in the hands of criminals and having been already misused via the sale of such information on the Internet black market;

d. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market; and

h. The loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

65. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

66. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

67. The substantial delay in providing notice of the Data Breach, and continuing to operate the compromised e-commerce website even after discovery of the malware infecting that site, deprived Plaintiff and the Class of the ability to promptly mitigate potential adverse consequences resulting from the Cyber-Attack. As a result of Defendants' delay in detecting and notifying consumers of the Cyber-Attack, the risk of fraud for Plaintiff and Class Members was and has been driven even higher.

CLASS ALLEGATIONS

68. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

69. Plaintiff proposes the following Class definitions, subject to amendment as

appropriate:

Nationwide Class:

All residents of the United States whose Private Information was compromised as a result of the Cyber-Attack first disclosed by PupBox in October 2020.

Washington Subclass:

All residents of Washington State whose Private Information was compromised as a result of the Cyber-Attack first disclosed by Pup Box in October 2020.

70. Excluded from each of the above Classes are Defendants and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its 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.

71. Each of the proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

72. **Numerosity.** The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 30,000 customers of Defendants whose data was compromised in the Cyber-Attack.

73. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

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 its 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 data breach to Plaintiff and Class Members;

f. Whether Defendants breached its duty to provide timely and accurate notice of the data breach to Plaintiff and Class Members;

g. Whether and when Defendants knew or should have known that Plaintiff's and Class Members' personal information entered into its computer systems for payment purposes was 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.

74. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Cyber-Attack.

75. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data breach class actions.

76. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members'

Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

77. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

78. 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.

79. 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
Violation of the Washington State Consumer Protection Act, RCW 19.86.010, *et seq*.
(On Behalf of Plaintiff and the Washington Subclass)

80. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

81. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

82. Defendants are each a "person" as described in RCW 19.86.010(1).

83. Defendants engage in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

84. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendants' practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

85. In the course of conducting their business, Defendants committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' Private Information, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

86. Defendants also violated the CPA by failing to timely notify and concealing from Plaintiff and Class Members regarding the unauthorized release and disclosure of their Private Information. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information and identities.

87. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendants' wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

88. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

89. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Cyber-Attack and its violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her Private Information; (5) deprivation of the value of his or her Private Information, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

90. Unless restrained and enjoined, Defendants will continue to engage in the

above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it.

91. Plaintiff, on behalf of herself and the Class Members, also seeks to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiff, on behalf of herself and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.

COUNT II
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices
(On Behalf of Plaintiff and the National Class)

92. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1–79 as if fully set forth herein. Plaintiff brings this claim on behalf of herself and the National Class.

93. Defendants have violated Cal. Bus. & Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200 with respect to the services provided to the National Class.

94. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described

herein; by soliciting and collecting Plaintiff's and Class Members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' Private Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the Private Information of Plaintiff and the Class Members.

95. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the Cyber-Attack in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

96. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiff and Class Members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

97. Defendants knew or should have known that Defendants' computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' Private Information and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

98. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class Members of money or property that Defendants may have acquired by means of Defendants' unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Civ. Proc. Code § 1021.5), and injunctive or other equitable relief.

COUNT III
Violation of the California Consumer Records Act,
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff and the National Class)

99. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1–79 as if fully set forth herein. Plaintiff brings this claim on behalf of herself and the National Class.

100. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

101. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

102. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

iv. The date of the breach;

v. The estimated date of the breach; or

vi. The date range within which the breach occurred.

103. The notification shall also include the date of the notice; whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; a general description of the breach incident, if that information is possible to determine at the time the notice is provided; and the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

104. The Cyber-Attack described herein constituted a "breach of the security system" of Defendants.

105. As alleged above, Defendants unreasonably delayed informing Plaintiff and Class Members about the Cyber-Attack, affecting their Private Information, after Defendants knew the Cyber-Attack had occurred.

106. Defendants failed to disclose to Plaintiff and Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendants knew or reasonably believed such information had been compromised.

107. Defendants' ongoing business interests gave Defendants incentive to conceal the Cyber-Attack from the public to ensure continued revenue.

108. Upon information and belief, no law enforcement agency instructed Defendants that timely notification to Plaintiff and Class Members would impede its

investigation.

109. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiff and Class Members were deprived of prompt notice of the Cyber-Attack and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class Members because their stolen information would have had less value to identity thieves.

110. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Cyber-Attack itself.

111. Plaintiff and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and Class Members as alleged above and equitable relief.

112. Defendants' misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiff and Class Members of "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c)(2) in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiff and Class Members and despicable conduct that has subjected Plaintiff and Class Members to hardship in conscious disregard of their rights. As a result, Plaintiff and Class Members are entitled to punitive damages against Defendants under Cal. Civ. Code § 3294(a).

Count IV
Negligence

(On behalf of Plaintiff, the Nationwide Class and the Washington Subclass)

113. Plaintiff realleges, as if fully set forth herein, the allegations of preceding paragraphs 1–79.

114. Defendants solicited, gathered, and stored personal information, including PCD, of Plaintiff and the Nationwide Negligence Class or, alternatively, the Separate Washington Negligence Subclass (collectively, the "Class" as used in this Count) to facilitate sales transactions.

115. Defendants knew, or should have known, of the risks inherent in collecting and storing the personal information of Plaintiff and the Class and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches by other national retailers.

116. Defendants owed duties of care to Plaintiff and the Class whose personal information was entrusted to it. Defendants' duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting personal information and PCD in its possession;

b. To protect customers' personal information and PCD using reasonable and adequate security procedures and systems that are compliant with the PCI-DSS standards and consistent with industry-standard practices;

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

d. To promptly notify Plaintiff and Class Members of the Data Breach.

117. By collecting and storing this data in its computer property, and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiff's and Class Members' Private Information held within it—to prevent disclosure of the Private Information, and to safeguard the Private Information from theft. Defendants' duties included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

118. Because Defendants knew that a breach of its systems would damage thousands of its customers, including Plaintiff and Class Members, it had a duty to adequately protect their personal information.

119. Defendants owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

120. Defendants knew, or should have known, that its computer systems did not adequately safeguard the personal information of Plaintiff and the Class.

121. Defendants breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the personal information of Plaintiff and the Class.

122. Defendants breached its duties of care by failing to provide prompt notice of the Data Breach to the persons whose personal information was compromised.

123. Defendants acted with reckless disregard for the security of the personal information of Plaintiff and the Class because Defendants knew or should have known that its computer systems and data security practices were not adequate to safeguard the personal information that that it collected and stored, which hackers were attempting to access.

124. Defendants acted with reckless disregard for the rights of Plaintiff and the Class by failing to provide prompt and adequate notice of the Data Breach so that they could take measures to protect themselves from damages caused by the fraudulent use the personal information compromised in the Data Breach.

125. Defendants had a special relationship with Plaintiff and the Class. Plaintiff's and the Class' willingness to entrust Defendants with their personal information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect its systems (and the personal information that it stored on them) from attack.

126. Defendants own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their personal information. Defendants' misconduct included failing to:

a. Secure its e-commerce website;

b. Secure access to its servers;

c. Comply with industry standard security practices;

d. Follow the PCI-DSS standards;

e. Encrypt PCD at the point-of-sale and during transit;

f. Employ adequate network segmentation;

g. Implement adequate system and event monitoring;

h. Utilize modern payment systems that provided more security against intrusion;

i. Install updates and patches in a timely manner; and

j. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

127. Defendants also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and the Class' personal information and promptly notify them about the Data Breach.

128. Defendants breached the duties it owed to Plaintiff and Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect their personal information both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the Data Breach; and

d. By failing to timely and accurately disclose that the personal information of Plaintiff and the Class had been improperly acquired or accessed.

129. But for Defendants' wrongful and negligent breach of the duties it owed Plaintiff and the Class Members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

130. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of further harm.

131. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was reasonably foreseeable.

132. The injury and harm that Consumer Plaintiff and Class Members suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct.

133. Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

Count V
Negligence *Per Se*
(On Behalf of Plaintiff and the National Class)

134. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

135. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the personal information, including PCD, of Plaintiff, the National Class, and the Washington Subclass ("the Classes," for purposes of this count).

136. The FTCA prohibits "unfair . . . practices in or affecting commerce,"

including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect personal information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

137. Defendants solicited, gathered, and stored personal information, including PCD, of Plaintiff and the Classes to facilitate sales transactions which affect commerce.

138. Defendants violated the FTCA by failing to use reasonable measures to protect personal information of Plaintiff and the Classes and not complying with applicable industry standards, as described herein.

139. Defendants' violation of the FTCA constitutes negligence per se.

140. Plaintiff and the Classes are within the class of persons that the FTCA was intended to protect.

141. The harm that occurred as a result of the Cyber-Attack is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Classes.

142. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Classes have suffered, and continue to suffer, injuries damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the data breach, including but not limited to late fees charges; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, inter alia, by contacting their financial institutions to place to dispute fraudulent charges, closing or modifying financial accounts, closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending.

143. Defendants breached its duties to Plaintiff and the Classes under these states' laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Classes' personal information.

144. Defendants' violation of the FTCA constitutes negligence *per se*.

145. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

146. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that it was failing to meet its duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

Count VI
Breach of Implied Contract
(On Behalf of Plaintiff, the National Class, and Washington Subclass)

148. Plaintiff realleges, as if fully set forth herein, the allegations of preceding paragraphs 1–79.

149. When Plaintiff and Members of the Nationwide Class and the Washington Subclass (collectively, the "Class" as used in this Count), provided their personal information to Defendants in making purchases on Defendants' website, 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.

150. Defendants invited its customers, including Plaintiff and the Class, to make purchases on Defendants' website using payment cards in order to increase sales by making purchases more convenient.

151. 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.

152. Based on this implicit understanding, Plaintiff and the Class accepted the offers and provided Defendants with their personal information by using their payment cards in connection with purchases on Defendants' website during the period of the Cyber-Attack.

153. Defendants manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiff's and Class Members' Private Information.

154. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

155. 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 a data breach.

156. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

157. 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 Data Breach.

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

Count VII

Unjust Enrichment

(On Behalf of Plaintiff, the National Class, and Washington Subclass)

159. Plaintiff realleges, as if fully set forth herein, the allegations of preceding paragraphs 1–79.

160. This Count is plead in the alternative to Count VI above.

161. Plaintiff and Members of the Nationwide Class and the Washington Subclass (collectively, the "Class" as used in this Count), conferred a monetary benefit on Defendants. Specifically, they made purchases from Defendants and provided Defendants with their personal information by using their payment cards for the purchases that they would not have made if they had known that Defendants did not provide adequate protection of their personal information.

162. 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.

163. Defendants failed to secure the Plaintiff's and Class Members' personal information, and therefore was unjustly enriched by the purchases made by Plaintiff and the Class that they would not have made had they known that Defendants did not keep their personal information secure.

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

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

166. 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 herself and the Classes described above, seeks the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the

undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Classes requested herein;

b. Judgment in favor of Plaintiff and the Classes awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

RESPECTFULLY SUBMITTED this 18th day of December, 2020.

HUSSIN LAW

/s/ *Tammy Hussin*
Tammy Hussin (CA Bar No. 155290)
1596 N. Coast Highway 101
Encinitas, CA 92024
Phone: (877)677-5397
Fax: (877)667-1547
tammy@hussinlaw.com

MASON LIETZ & KLINGER LLP

/s/ *Gary E. Mason*
Gary E. Mason* (DC Bar No. 418073)
David K. Lietz* (DC Bar No. 430557)
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Phone: (202) 429-2290
Fax: (202) 429-2294
gmason@masonllp.com
dlietz@masonllp.com

MASON LIETZ & KLINGER LLP

/s/ *Gary M. Klinger*
Gary M. Klinger* (IL Bar No. 6303726)
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (202) 429-2290
Fax: (202) 429-2294
gklinger@masonllp.com

Attorneys for Plaintiff and the Proposed Classes

* Applications for admission *pro hac vice* to be filed