BETSY C. MANIFOLD (182450)
manifold@whafh.com
RACHELE R. BYRD (190634)
byrd@whafh.com
MARISA C. LIVESAY (223247)
livesay@whafh.com
BRITTANY N. DEJONG (258766)
dejong@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599

M. ANDERSON BERRY (262879)
aberry@justice4you.com
LESLIE GUILLON (222400)
lguillon@justice4you.com
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CHERYL GASTON and RENATE GARRISON, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

FABFITFUN, INC.,

Defendant.

Case No. 2:20-cv-09534-RGK-E

FIRST AMENDED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Cheryl Gaston and Renate Garrison ("Plaintiffs"), individually and on behalf of themselves and all other persons similarly situated, bring this Class Action Complaint against FabFitFun, Inc. ("FabFitFun" or "Defendant") and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. FabFitFun is a popular lifestyle e-commerce retailer best known for its flagship product, the FabFitFun Box. The FabFitFun Box includes a selection of full-size products across beauty, fashion, fitness, wellness, home, and technology – delivered each season. In addition to the Box, FabFitFun members receive, among other things, access to FabFitFunTV, a streaming video service that offers on-demand wellness content, the FabFitFun online Community, and members-only shopping experiences. Defendant sells its memberships online through its website and uses an e-commerce platform to take customers' personal and payment information.

2. On or about September 18, 2020, FabFitFun began notifying customers and state Attorneys General about a widespread data breach that occurred from April 26, 2020 to May 14, 2020 and May 22, 2020 to August 3, 2020 (the "Data Breach"). Hackers not only "scraped" many of Defendant's customers' full names from the website by infecting it with a malicious code, hackers also stole customers' personally identifiable information ("PII"), including names, email addresses, FabFitFun account passwords, shipping and billing addresses, payment card account numbers, card expiration dates, and card verification codes. The hackers got everything they needed to illegally use FabFitFun customers' payment cards to make fraudulent purchases and to steal customers' identities. Defendant is offering affected customers one year of identity protection services and a $25 credit, which requires a current FabFitFun membership and expires by the end of the year.

3. All of this PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to its failure to prevent the Data Breach, Defendant failed to detect and report the breach for months.

4. According to FabFitFun, on August 7, 2020 its "technical team" discovered that an unauthorized third party inserted malicious code on portions of its website that "may have enabled them to capture certain information in connection with customer sign ups." Defendant claims it removed the malicious code and took steps to secure its website with the help of forensic cyber security experts engaged to assist with its investigation.

5. Defendant did not begin notifying affected customers and states' Attorneys General until over a month later, on or about September 18, 2020.

6. The stolen PII has great value to hackers due to its thoroughness and the numbers involved. It is likely that hackers stole the full payment card information for hundreds of thousands of customers. For example, the Maine Attorney General reports that the Data Breach affected 209,984 persons.[1]

7. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect its users' PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor its website and e-commerce platform for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

8. Plaintiffs and similarly situated customers ("Class members") have suffered injury as a result of Defendant's conduct. These injuries may include: (i) lost or diminished value of their PII; (ii) out-of-pocket expenses associated with

[1] *See Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/f5a80de8-c712-4ddf-9544-480f9f1f81e9.shtml (last visited Dec. 23, 2020).

the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under (a) the Colorado Security Breach Notification Act, Colo. Rev. Stat. § 6-1-716, *et seq*., (b) the Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq*., (c) the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. § 646.605, *et seq*.; and (v) the continued and certainly increased risk to their PII, which (a) may remain available on the dark web for individuals to access and abuse, and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

JURISDICTION & VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Moreover, this Court has jurisdiction over this action under 28 U.S.C. § 1332(a)(1) because Plaintiff Gaston is a Colorado citizen and Plaintiff Garrison is an Oregon citizen and therefore diverse from Defendant, which is not a citizen of Colorado or Oregon.

10. This Court has personal jurisdiction over Defendant because Defendant has systematic and continuous contacts with the state through its website and because its headquarters are located here.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

12. Plaintiff Cheryl Gaston is a citizen of Colorado residing in Colorado Springs. Ms. Gaston purchased a subscription on FabFitFun's website on May 7, 2020 using her debit card. She received FabFitFun's Notice of Data Breach or about September 29, 2020.

13. Plaintiff Renate Garrison is a citizen of Oregon residing in Portland. Ms. Garrison made purchases from FabFitFun's website on June 28, 2020 and July 18, 2020, using her credit card. She received FabFitFun's Notice of Data Breach or about September 29, 2020.

14. Defendant FabFitFun is a Delaware corporation with its principal place of business in Los Angeles, California. During the class period, FabFitFun operated across the United States through its websites.

SUBSTANTIVE ALLEGATIONS

FabFitFun's Background

15. Initially founded in 2010 as an online magazine focused on beauty, fitness and fashion, FabFitFun expanded into subscription box marketing three years later – an industry that has grown at a compound annual growth rate of nearly 60 percent. Defendant claims to now have more than 1 million members worldwide. Its main offering is its FabFitFun Box, a curated collection of products across beauty, fashion, wellness, fitness, home and technology categories delivered four times per year. The box is priced at $50 per season or $180 per year. FabFitFun annual revenues are estimated at $300 million.

16. Defendant assures its customers that it is concerned about PII security and claims: "We take reasonable and appropriate measures to help keep information secure and to help prevent it from becoming disclosed."[2]

[2] *See Privacy Policy* (effective Feb. 28, 2020 to Sept. 28, 2020), FABFITFUN, INC., https://legal.fabfitfun.com/#privacy-policy-v1 (last visited Dec. 23, 2020).

17. Defendant does not claim that it abides by the Payment Card Industry Data Security Standard ("PCI DSS") compliance, which is a requirement for businesses that store, process, or transmit payment card data.

18. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions. Businesses that fail to maintain PCI DSS compliance are subject to steep fines and penalties.

19. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks using anti-virus software and updating it regularly.

20. To purchase items on Defendant's website, customers can either create an account or check out as a guest. Either choice requires, at a minimum, that the customer enter the following PII onto the website:

- Name;
- billing address;
- shipping address;
- email address;
- FabFitFun account password (if applicable);
- name on the payment card;
- type of payment card;
- full payment card number;
- payment card expiration date; and
- security code or CVV code (card verification number).

21. During the relevant period, when a customer purchased items on Defendant's website, as a guest or through an account, there was no reference to the "Privacy Policy," and customers were not required to read or check a box

acknowledging having reviewed the "Terms of Use" to make a purchase. Links to FabFitFun's "Privacy Policy" were included only at the extreme bottom border of the website pages in black, unremarkable font, with no clear indications of hyperlinks to the policies or terms.

The Data Breach

22. Starting on or about September 18, 2020, FabFitFun notified customers via email and on or about September 22, 2020, mailed customers a Notice of Data Breach. FabFitFun's co-founder and co-CEO, Michael Broukhim, informed FabFitFun's affected customers that:

> ***What Happened?***
>
> Our technical team recently discovered that an unauthorized third party inserted malicious code on portions of our website that may have enabled them to capture certain information in connection with customer sign ups. Based on our forensic investigation, this incident concerns the new member sign up pages of our website during the period between April 26, 2020 and May 14, 2020, and between May 22, 2020 and August 3, 2020. According to our records, you signed up for FabFitFun during this timeframe, and your information therefore could have been affected. Although we believe that only a subset of members who signed up during this period were affected, we are notifying everyone that signed up during this timeframe as a precaution.
>
> ***What Information was Involved?***
>
> This incident would have involved emails and FabFitFun passwords for customers that signed up using PayPal or Apple Pay. For customers using credit or debit cards, the information involved would also have included name, address, payment card account number, card expiration

date, and card verification code.[3]

* * *

23. Defendant's notice to the state Attorneys General also provided this same information.[4]

24. Defendant admits that it did not detect the Data Breach. FabFitFun's customers' information was scraped by hackers and available to other criminals and, on information and belief, may still be for sale to criminals on the dark web. Defendant failed to use encryption to protect sensitive information transmitted online, and unauthorized individuals accessed Defendant's customers' unencrypted, unredacted information, including name, address, email address, account password, and payment card information, which includes payment card number, CVV code, expiration date, and possibly more.

Scraping and E-Skimming Breaches

25. Magecart is a loose affiliation of hacker groups responsible for skimming payment card attacks on various companies, including British Airways and Ticketmaster. Typically, these hackers insert virtual credit card skimmers or scrapers (also known as formjacking) into a web application (usually the shopping cart), and proceed to scrape credit card information to sell on the dark web.

26. The hackers target what they refer to as the *fullz* – a term used by criminals to refer to stealing the full primary account number, card holder contact information, credit card number, CVC code, and expiration date. The *fullz* is exactly what FabFitFun admits the malware infecting its e-commerce platform scraped.

27. These cyber-attacks exploit weaknesses in the code of the e-commerce platform, without necessarily compromising the victim website's network or server.

28. Magecart and these scraping breaches are not new: RiskIQ's earliest

[3] *See* Exhibit A attached hereto.

[4] *See* Exhibit B attached hereto.

Magecart observation occurred on August 8th, 2010. Thus, Defendant would have been made aware of this type of breach since that time, especially considering the surge of these types of breaches in the last few years.

29. Unfortunately, despite all of the publicly available knowledge of the continued compromises of PII in this manner, Defendant's approach to maintaining the privacy and security of Plaintiffs' and Class members' PII was negligent, or, at the very least, Defendant did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect their customers' valuable PII.

Value of Personally Identifiable Information

30. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit or debit card number can sell for $5-110 on the dark web; the *fullz* sold for $30 in 2017. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

31. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach. Defendant were, or should have been, fully aware of the significant volume of daily credit and debit card transactions on its website – the malware infected FabFitFun e-commerce as its retail locations closed and customers could only get FabFitFun products from Defendant's website – amounting to potentially hundreds of thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

Plaintiff Gaston's Experience

32. Plaintiff Gaston purchased a subscription for $41.55 from FabFitFun's website on May 7, 2020, using her debit card.

33. On the payment platform, Ms. Gaston entered her PII: name, billing/shipping address, payment card type and full number, CVV security code, payment card expiration date, and email address.

34. During this transaction, Ms. Gaston was not asked to read or expressly "agree" to FabFitFun's "Terms of Use and Sale," "Privacy Policy," or the "FabFitFun Membership Terms."

35. On or about September 29, 2020, FabFitFun notified Ms. Gaston by U.S. Mail of the Data Breach in the Notice of Data Breach. FabFitFun admitted that the Data Breach "would have involved emails and FabFitFun passwords," along with full name, address, payment card type and full number, CVV security code, and payment card expiration date.

36. In response to the Notice of Data Breach, Ms. Gaston had to spend time dealing with the consequences of the Data Breach, which includes time reviewing the account compromised by the Data Breach, contacting her bank, exploring credit monitoring options, and self-monitoring her accounts. This is time Ms. Gaston otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

37. Knowing that the hacker stole her PII, and that her PII may be available for sale on the dark web, has caused Ms. Gaston anxiety. She is now very concerned about credit card theft and identity theft in general. This breach has given Ms. Gaston hesitation about using FabFitFun's services, and reservations about shopping on other online websites.

38. Now, due to Defendant's misconduct and the resulting Data Breach, hackers obtained her PII at no compensation to Ms. Gaston whatsoever. That is money lost for her, and money gained for the hackers, who could sell her PII on the

dark web.

39. Ms. Gaston also suffered actual injury and damages in paying money to, and purchasing products from, Defendant's website during the Data Breach, expenditures which she would not have made had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

40. Moreover, Ms. Gaston suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

41. Plaintiff Gaston has a continuing interest in ensuring her PII, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Gaston's Efforts to Secure PII

42. Defendant's Data Breach caused Ms. Gaston harm.

43. Prior to the activity described above during the period in which the Data Breach occurred, the debit card that Ms. Gaston used to purchase products on Defendant's website had never been stolen or compromised. Ms. Gaston reviewed her credit reports and other financial statements routinely and to her knowledge this card had not been compromised in any manner.

44. Additionally, Ms. Gaston never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

45. Ms. Gaston stores any and all hardcopy and electronic documents containing her PII in a safe and secure location.

Plaintiff Garrison's Experience

46. Plaintiff Garrison purchased an item on FabFitFun's website for $5.00 on June 28, 2020, using her credit card. On July 18, 2020, she purchased a year subscription to FabFitFun on its website for $179.99, using the same credit card.

47. On the payment platform, Ms. Garrison entered her PII: name,

billing/shipping address, payment card type and full number, CVV security code, payment card expiration date, and email address.

48. During this transaction, Ms. Garrison was not asked to read or expressly "agree" to FabFitFun's "Terms of Use and Sale," "Privacy Policy," or the "FabFitFun Membership Terms."

49. On or about September 29, 2020, FabFitFun notified Ms. Garrison by U.S. Mail of the Data Breach. FabFitFun admitted that the Data Breach "would have involved emails and FabFitFun passwords," along with full name, address, payment card type and full number, CVV security code, and payment card expiration date.

50. On or about August 19, 2020, unknown third parties used Ms. Garrison's credit card, the same card she used on FabFitFun's website, to make an unauthorized purchase on Amazon.com. On or about August 20, 2020, her credit card company confirmed that the purchase was fraudulent.

51. To protect Ms. Garrison's credit and debit cards, her bank issued new cards in late August 2020. Ms. Garrison was unable to use her credit and debit cards for approximately two weeks before each card was replaced by mail. She was forced to use alternative methods of payment and was deprived of rewards and monetary dividends.

52. In response to the Notice of Data Breach and the fraud, Ms. Garrison had to spend time dealing with the consequences, which included time reviewing the account compromised by the Data Breach, contacting her bank, exploring credit monitoring options, and self-monitoring her accounts. Ms. Garrison also contacted FabFitFun to confirm the scope of the Data Breach, but she was initially ignored. Ms. Garrison called, emailed and initiated "chat" sessions through FabFitFun's website. Before getting a response, she also used Twitter to get FabFitFun's attention. Eventually, she communicated with a FabFitFun representative. This is time Ms. Garrison otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

53. Knowing that the hacker stole her PII, and that her PII may be available for sale on the dark web, has caused Ms. Garrison anxiety. She is now very concerned about credit card theft and identity theft in general. This breach has given Ms. Garrison hesitation about shopping on other online websites.

54. Now, due to Defendant's misconduct and the resulting Data Breach, hackers obtained Ms. Garrison's PII at no compensation to her whatsoever. That is money lost for her, and money gained for the hackers, who could sell her PII on the dark web.

55. Moreover, Ms. Garrison suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

56. Plaintiff Garrison has a continuing interest in ensuring her PII, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Garrison's Efforts to Secure PII

57. Defendant's Data Breach caused Ms. Garrison harm.

58. Prior to the activity described above during the period in which the Data Breach occurred, the credit card that Ms. Garrison used to purchase products on Defendant's website had never been stolen or compromised.

59. Additionally, Ms. Garrison never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

60. Ms. Garrison shreds any and all hardcopy documents containing her PII or stores them in a safe and secure location.

CLASS ACTION ALLEGATIONS

61. Plaintiffs bring this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, on behalf of themselves and on behalf of all members of the following class:

All individuals whose PII was compromised in the data breach

announced by FabFitFun on or about September 18, 2020 (the "Class").

62. The Colorado Subclass is defined as follows:

All persons residing in Colorado whose PII was compromised in the data breach announced by FabFitFun on September 18, 2020 (the "Colorado Subclass").

63. The Oregon Subclass is defined as follows:

All persons residing in Oregon whose PII was compromised in the data breach announced by FabFitFun on September 18, 2020 (the "Oregon Subclass").

The Class and Subclasses together are referred to herein as the "Classes."

64. Excluded from the Classes are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

65. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

66. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of customers whose PII may have been improperly accessed in the data breach, and the Classes are apparently identifiable within Defendant's records.

67. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class members. These include:

a. When Defendant actually learned of the data breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class members' PII;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class members' PII;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and Class members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

h. Whether Defendant caused Plaintiffs and Class members damages;

i. Whether Defendant violated the law by failing to promptly notify Class members that their PII had been compromised;

j. Whether Plaintiffs and the other Class members are entitled to credit monitoring and other monetary relief;

k. Whether Defendant violated the Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*;

l. Whether Defendant violated the Colorado Security Breach Notification Act, Colo. Rev. Stat. § 6-1-716, *et seq.*; and

m. Whether Defendant violated the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. § 646.605, *et seq*.

68. **Typicality**: Plaintiffs' claims are typical of those of other Class members because all had their PII compromised as a result of the Data Breach, due

to Defendant's misfeasance.

69. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Class members. Plaintiffs' Counsel are competent and experienced in litigating privacy-related class actions.

70. **Superiority and Manageability**: Under Rule 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

71. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant has acted or 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.

72. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and

applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach; and

e. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class)

73. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 72.

74. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

75. The legal duties owed by Defendant to Plaintiffs and Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and Class members in its possession;

b. To protect PII of Plaintiffs and Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class members of the Data Breach.

76. Defendant's duty to use reasonable data security measures also arose

under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendant.

77. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiffs and Class members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

78. Defendant breached their duties to Plaintiffs and Class members. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the facts that "scraping" hacks have been surging since 2016.

79. Defendant knew or should have known that their security practices did not adequately safeguard Plaintiffs' and the other Class members' PII, including, but not limited to, the failure to detect the malware infecting Defendant's e-commerce platform for months.

80. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiffs and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PII during the period it was within Defendant's possession and control.

81. Defendant breached the duties it owed to Plaintiffs and Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards

during the period of the data breach (e.g., There is no indication that Defendant's e-commerce platform is PCI DSS compliant and encrypts customers' order information, such as name, address, and credit card number, during data transmission, which did not occur here);

c. Failing to act despite knowing or having reason to know that Defendant's systems were vulnerable to e-skimming or similar attacks (e.g., Defendant did not detect the malicious code on the e-commerce platform, nor did it implement safeguards in light of the surge of e-skimming attacks on retailers); and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

82. Due to Defendant's conduct, Plaintiffs and Class members are entitled to credit monitoring. Ongoing credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class members. Hackers not only "scraped" many of FabFitFun customers' names from the website, they also stole customers' billing and shipping addresses, email addresses, account passwords, payment card numbers, CVV codes, and payment card expiration dates. They got the *fullz* – everything they need to illegally use FabFitFun customers' credit cards to make illegal purchases. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

83. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

84. As a result of Defendant's negligence, Plaintiffs and Class members

suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession, subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; and (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiffs and Class members, including ongoing credit monitoring.

85. These injuries were reasonably foreseeable given the history of security breaches of this nature since 2016. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendant's negligent conduct.

SECOND CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

86. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 72.

87. Defendant owes duties of care to Plaintiffs and Class members which would require it to adequately secure PII.

88. Defendant still possesses PII regarding Plaintiffs and Class members.

89. Although FabFitFun claims it "takes the security of personal information very seriously," is "continuing to review and enhance our security

measures," and is "confident that the issue has been resolved and will no longer affect transactions on our website" (*see* Ex. A at 1-2), there is no detail on what, if any, fixes have really occurred.

90. Plaintiffs and Class members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

91. There is no reason to believe that Defendant's security measures are any more adequate than they were before the breach to meet Defendant's contractual obligations and legal duties, and there is no reason to think Defendant has no other security vulnerabilities that have not yet been knowingly exploited.

92. Plaintiffs, therefore, seek a declaration that (1) Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised,

hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and securing checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Class members for a period of ten years; and

h. Meaningfully educating its users about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendant's customers must take to protect themselves.

THIRD CLAIM FOR RELIEF

Violations of the Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*

(On Behalf of Plaintiff Gaston and the Colorado Subclass)

93. Plaintiff Gaston re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 72.

94. Defendant is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

95. Defendant engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

96. Plaintiff Gaston and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Defendant or successors in interest to actual consumers.

97. Defendant engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Knowingly making a false representation as to the characteristics of services;

b. Representing that services are of a particular standard, quality, or grade, though Defendant knew or should have known that they were of

another;

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

d. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

98. Defendant's deceptive trade practices include:

a. Falsely representing to its customers that it would employ reasonable security and privacy measures;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Gaston and Colorado Subclass members' PII, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Gaston and Colorado Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Gaston's and Colorado Subclass members' PII, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Gaston's and Colorado Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not

reasonably or adequately secure Plaintiff Gaston's and Colorado Subclass members' PII; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Gaston's and Colorado Subclass members' PII.

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

100. Defendant intended to mislead Plaintiff Gaston and Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

101. Had Defendant disclosed to Plaintiff Gaston and Subclass members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as a maintaining a secure e-commerce platform and was trusted with sensitive and valuable PII regarding hundreds of thousands of consumers, including Plaintiff and the Colorado Subclass.

102. Defendant acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff Gaston's and Colorado Class members' rights.

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

104. Plaintiff Gaston and Colorado Subclass members seek all monetary and nonmonetary relief allowed by law, including the greater of: (a) actual damages, or

(b) $500, or (c) three times actual damages (for Defendant's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

FOURTH CLAIM FOR RELIEF
Violations of the Colorado Security Breach Notification Act, Colo. Rev. Stat. § 6-1-716, *et seq.*
(On Behalf of Plaintiff Gaston and the Colorado Subclass)

105. Plaintiff Gaston re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 72.

106. Defendant is a business that owns or licenses computerized data that includes PII as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

107. Plaintiff Gaston and Colorado Subclass members' PII includes PII as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

108. Defendant is required to accurately notify Plaintiffs and Colorado Subclass members if it becomes aware of a breach of its data security system **in the most expedient time possible** and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

109. Because Defendant was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

110. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Colo. Rev. Stat. § 6-1-716(2).

111. As a direct and proximate result of Defendant's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff Gaston and Colorado Subclass members suffered damages, as described above.

112. Plaintiff Gaston and Colorado Subclass members seek relief under

Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

FIFTH CLAIM FOR RELIEF
Violations of the Oregon Unlawful Trade Practices Act,
Or. Rev. Stat. § 646.605, *et seq.*
(On Behalf of Plaintiff Garrison and the Oregon Subclass)

113. Plaintiff Garrison re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 72.

114. Defendant is a "person," as defined by Or. Rev. Stat. § 646.605(4).

115. Defendant engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

116. Defendant sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

117. Defendant advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

118. Defendant engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

a. Represented that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

b. Represented that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

c. Advertised its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and

d. Concurrent with tender or delivery of its goods and services, failed to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

119. Defendant's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Garrison and Oregon Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Garrison and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. § 646A.600, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Garrison and Oregon Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Garrison and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. § 646A.600, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Garrison and Oregon

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Garrison and Oregon Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. § 646A.600, *et*

seq.

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

121. Defendant intended to mislead Plaintiff Garrison and Oregon Subclass members and induce them to rely on its misrepresentations and omissions. Had Defendant disclosed to Plaintiff Garrison and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff Garrison's and Class members' PII as part of the services Defendant provided and for which Plaintiff Garrison and Class members paid without advising Plaintiff Garrison and Class members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff Garrison's and Class members' PII. Accordingly, Plaintiff Garrison and the Oregon Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

122. Defendant acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff Garrison and Oregon Subclass members' rights. Recent, frequent, and strikingly similar data breaches within the industry put Defendant on notice that its security and privacy protections were inadequate.

123. As a direct and proximate result of Defendant's unlawful practices, Plaintiff Garrison and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses

from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

124. Plaintiff Garrison and Oregon Subclass members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all of the members of the Classes, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

A. For an Order certifying the Classes as defined herein and appointing Plaintiffs and their Counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Classes members' PII;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and class members unless

Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and class members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiffs' and class members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training

program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and class members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third

party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For restitution and disgorgement of the revenues wrongfully obtained as a result of Defendant's wrongful conduct;

E. For an award of actual damages, statutory damages and compensatory damages, in an amount to be determined at trial;

F. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

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

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a jury trial for all claims so triable.

DATED: January 29, 2021

CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.

By: */s/M. Anderson Berry*
M. ANDERSON BERRY

M. ANDERSON BERRY (262879)
aberry@justice4you.com
LESLIE GUILLON (222400)
lguillon@justice4you.com
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
BETSY C. MANIFOLD
manifold@whafh.com

RACHELE R. BYRD
byrd@whafh.com
MARISA C. LIVESAY
livesay@whafh.com
BRITTANY N. DEJONG
dejong@whafh.com
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599

Counsel for Plaintiffs