M. Anderson Berry, SBN 262879
aberry@justice4you.com
Leslie Guillon, SBN 222400
lguillon@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

John A. Yanchunis (*Pro Hac Vice* Forthcoming)
jyanchunis@ForThe People.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

BERNADETTE BARNES, an individual and California resident, on behalf of herself and all others similarly situated,

Plaintiff,

vs.

HANNA ANDERSSON, LLC, and SALESFORCE.COM, INC.

Defendants.

Case No.:

CLASS ACTION COMPLAINT

1.) Negligence

2.) Declaratory Relief

3.) Violation of the California Unfair Competition Law, Business & Professions Code § 17200, *et seq*.

DEMAND FOR JURY TRIAL

Plaintiff Bernadette Barnes brings this Class Action Complaint against Hanna Andersson, LLC ("Hanna") and Salesforce.com, Inc. ("Salesforce")(collectively, "Defendants"), on behalf of herself and all others similarly situated, and allege, upon personal

knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Hanna Andersson specializes in selling high-end children's apparel through its popular website and specialty retail stores throughout the United States. For online sales, Hanna uses a third-party ecommerce platform to take customers' personal and payment information. The ecommerce platform is supplied to Hanna by Salesforce's Commerce Cloud Unit.

2. On January 15, 2020, Hanna Andersson notified customers and state Attorneys General about a widespread data breach that occurred from September 16, 2019 to November 11, 2019. Hackers not only "scraped" many of Hanna's customers' names from the website by infecting it with malware, they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and credit card expiration dates. The criminals got everything they needed to illegally use Hanna's customers' credit cards to make fraudulent purchases, and to steal the customers' identities.

3. Not only did hackers skim this personally identifiable information ("PII"), law enforcement found the stolen names and card information for sale on the dark web. That means the breach worked. Hackers accessed and then offered for sale the unencrypted, unredacted stolen PII to criminals. Because of Defendants' breach, customers' PII is still available on the dark web for criminals to access and abuse. Hanna's customers face a lifetime risk of identity theft.

4. This PII was compromised due to Hanna's and Salesforce's negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to their failure to prevent the breach, Hanna and Salesforce failed to detect the breach for almost three months.

5. Neither Hanna nor Salesforce had any idea the breach was happening. Months after it started, law enforcement found the stolen information on the dark web and warned Hanna on December 5, 2019. Hanna then investigated the breach, confirmed that Salesforce Commerce Cloud's ecommerce platform was "infected with malware," and confirmed that the PII entered by customers into the platform during the purchase process was "scraped"; that is, customers' PII was stolen from Hanna's website by unknown individuals, then sold on the dark web.

6. Hanna did not tell customers or the Attorneys General about this theft until over another month later, on January 15, 2020. To this day, Salesforce has not released a vulnerabilities and exposures report, nor has Salesforce made any notifications of the breach.

7. The stolen PII has great value to hackers due to the numbers involved: It is likely that tens of thousands of people – residents of every state – were affected by this breach. For example, Hanna states that almost 9,000 Washington residents may have been affected. On information and belief, over 10,000 California residents were affected.

8. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect its users' PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor Hanna's website and ecommerce platform for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates several California statutes.

9. Plaintiff and similarly situated Hanna customers ("Class members") have suffered injury as a result of Defendants' conduct. These injuries may include: (i) 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 lost time, (iv) deprivation of rights they possess under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200) and California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*.); (v) the continued and certainly an increased risk to their PII, which (a) remains available on the dark web for individuals to access and abuse, and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

II. PARTIES

10. Plaintiff Bernadette Barnes is a citizen of California residing in Sacramento County. Plaintiff Barnes purchased items from Hanna's website between September 16, 2019 and November 11, 2019. She received Hanna's notice of the data breach, dated January 15, 2020, on or about January 20, 2020.

11. Defendant Hanna Andersson, LLC is a Delaware Foreign Limited Liability Company with its principal place of business located at 1010 Northwest Flanders Street, Portland, Oregon. During the class period, Hanna operated in California through its website, and has multiple retail locations, including in Palo Alto and Walnut Creek, California.

12. Defendant Salesforce.com, Inc. is incorporated in Delaware with its principle place of business located at 1 Market Street, San Francisco, California. According to Hanna, during the class period, Salesforce supplied Hanna with cloud-based online ecommerce services through its Salesforce Commerce Cloud Unit.[1]

III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under 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 Hanna. Moreover, Plaintiff Barnes is a citizen of California and therefore diverse from Hanna, which is headquartered in Oregon with a Delaware LLC.

14. This Court has personal jurisdiction over Defendants because Salesforce is headquartered in California and conducts business in the state of California, and because Hanna has physical locations throughout California and conducts business in California through its website.

15. 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. Venue is also proper because Salesforce's terms of service require

[1] *See, e.g.*, Hanna Andersson's *Notification of Security Incident* to the Washington Attorney General, January 15, 2020, *available at*: https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/HannaAnderssonLLC.2020-01-15.pdf (last accessed Jan. 29, 2019); *see also*, Hanna Andersson's *Notification of Security Incident* to the California Attorney General, in part, January 15, 2020, *available at*: https://oag.ca.gov/system/files/Hanna_Multi-State%20Master__Rev1.pdf (last accessed Jan. 29, 2019).

that claims are resolved in "the courts located in San Francisco, California."[2]

IV. FACTUAL ALLEGATIONS

Background

16. Hanna has sold high-end children's clothing through mail order and retail stores since 1983. The company mostly sells clothing for babies through preteens, but recently added a women's collection and home furnishings. The company has expanded to over 60 retail locations across the United States, with an extensive presence online at www.hannaandersson.com. The company's annual sales are estimated to be over $140 million.

17. Salesforce is primarily a cloud technology[3] service as a software ("SaaS") company specializing in "customer relationship management" ("CRM"). According to Salesforce, CRM "is a technology for managing all your company's relationships and interactions with customers and potential customers." Due to the increase of cloud technology use, Salesforce's recent third quarter revenue of $4.5 billion was up 33 percent year over year.

18. As of 2020, Salesforce has multiple different cloud platforms: service cloud, marketing cloud, health cloud, app cloud, community cloud, analytics cloud, IoT cloud, Chatter cloud, Heroku engagement cloud, and the Salesforce Commerce Cloud.

19. The Salesforce Commerce Cloud provides a cloud-based unified ecommerce platform, or platform as a service ("PaaS"), with mobile, AI personalization, order management capabilities, and related services for business to customer ("B2C") and business to business ("B2B") companies.

20. Practically, businesses use Salesforce Commerce Cloud to provide websites to their customers who purchase items online. Salesforce's platform takes the key payment and personal information from the customer to finalize the transaction: name, billing and shipping addresses, payment card type and number, CVV (security) code, credit card expiration date, and

---

[2] *Terms of Service*, Salesforce.com, Inc., *available at* https://www.salesforce.com/company/legal/sfdc-website-terms-of-service/# (last accessed Jan. 29, 2019).

[3] As the name suggests, "cloud" technology is located remotely (in a "cloud computing platform" established by the vendor) and is accessed by the customer via the internet.

sometimes email address and telephone number.

21. Retailers and customers demand security to safeguard PII. Salesforce touts the secure nature of its PaaS ecommerce platform on its website:

- "Security protocols and infrastructure are constantly analyzed and updated to address new threats";
- "Some of the world's largest companies moved their applications to the cloud with Salesforce after rigorously testing the security and reliability of our infrastructure";
- "The cloud is used to back up data, deliver software, and provide extra processing capacity in a secure, scalable way";
- "[C]loud data is probably more secure than information stored on conventional hard drives";
- "With cloud services, information is encrypted and backed up continuously. Vendors monitor systems carefully for security vulnerabilities"; and
- "With PaaS, the vendor takes care of back-end concerns such as security, infrastructure, and data integration so users can focus on building, hosting, and testing apps faster and at lower cost."[4]

22. Hanna also ensures its customers that it's concerned about PII security:

> The security of your personal information is very important to Hanna, and we have implemented measures to ensure your information is processed confidentially, accurately, and securely. Our website is PCI DSS compliant and uses SSL/TLS (Secure Sockets Layer) technology to encrypt your order information, such as your name, address, and credit card number, during data transmission. We use a third-party payment processor, which is also PCI DSS compliant.[5]

---

[4] *What Is Cloud Computing?*, Salesforce.com, Inc., *available at*: https://www.salesforce.com/products/platform/best-practices/cloud-computing/?d=70130000000i88b (last accessed on Jan. 29, 2020).

[5] *Privacy Statement*, Hanna Andersson, LLC, *available at*: https://www.hannaandersson.com/security-and-privacy.html# (last accessed Jan. 29, 2020). When a customer purchases items on Hanna Andersson's website, as a guest or through an account, they are **not** asked to acknowledge the "Privacy Statement," and they are not expressly asked to agree to "Terms of Use" or "Terms of Service."

23. The PCI DSS (Payment Card Industry Data Security Standard) compliance is a requirement for businesses that store, process, or transmit payment card data. 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.

24. 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.[6]

25. To purchase items on Hanna'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;
- telephone number;
- email address;
- name on the credit card;
- type of credit card;
- full credit card number;
- credit card expiration date; and
- security code, or CVV code (card verification number).

26. At no time during the checkout process does Hanna require customers to expressly agree to the "Terms of Use."

The Data breach

27. On or about January 15, 2020, Hanna sent customers a *Notice of Security*

[6] PCI Security Standards Council, *available at*: https://www.pcisecuritystandards.org/ (last accessed Jan. 30, 2020).

Incident.[7] Hanna's President and CEO, Mike Edwards, informed the recipients of the notice that:

> **WHAT HAPPENED**
> Law enforcement recently notified Hanna Andersson that it had obtained evidence indicating that an unauthorized third party had accessed information entered on Hanna Andersson's website during purchases made between September 16 and November 11, 2019[….]
>
> **WHAT INFORMATION WAS INVOLVED**
> The incident potentially involved information submitted during the final purchase process on our website, www.hannaandersson.com, including name, shipping address, billing address, payment card number, CVV code, and expiration date.[8]

28. On that same day, January 15, 2020, Hanna's counsel at Perkins Coie in Seattle, Washington, mailed a different *Notification of Security Incident* to the Attorneys General of the states where affected customers reside, including California.[9] That notice included as an enclosure a sample of the notice that was sent to customers that same day.[10]

29. In the notice sent to the Attorneys General, there was much more information:

> **On December 5, 2019**, law enforcement informed Hanna Andersson that **credit cards used on its website were available for purchase on a dark web site**. Hanna Andersson immediately launched an investigation. **The investigation has confirmed that Hanna Andersson's third-party ecommerce platform, Salesforce Commerce Cloud, was infected with malware that may have scraped information entered by customers** into the platform during the purchase process. The earliest potential date of compromise identified by forensic investigators is September 16, 2019, and the malware was removed on November 11, 2019.
> …
> Hanna Andersson is cooperating with law enforcement and the payment card brands in their investigation of and response to the incident. It has taken **steps to re-secure** the online purchasing platform on its website and to **further harden it against compromise, including increasing use of multi-factor authentication**

---

[7] Hanna Andersson's *Notification of Security Incident*, January 15, 2020, archived by the California Attorney General, *available at*: https://oag.ca.gov/system/files/Hanna_Multi-State%20Master__Rev1.pdf (last accessed Jan. 29, 2019).

[8] *Id*.

[9] Hanna Andersson's *Notification of Security Incident* to the Washington Attorney General, January 15, 2020, *available at*: https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/HannaAnderssonLLC.2020-01-15.pdf (last accessed Jan. 29, 2019).

[10] Hanna Andersson's *Notification of Security Incident* to the California Attorney General, in part, January 15, 2020, *available at*: https://oag.ca.gov/system/files/Hanna_Multi-State%20Master__Rev1.pdf (last accessed Jan. 29, 2019).

and enhanced system monitoring (emphasis added).

30. The notice sent to Attorneys General states that law enforcement did not inform Hanna about its customers' credit cards being offered for sale on the "dark web" until December 5, 2019. At that time, Hanna "launched an investigation." The date the infecting malware was supposedly removed from Salesforce's "third-party ecommerce platform," however, was over three weeks *before* Hanna claims it found out about the breach.

31. Hanna admits it did not detect this breach on its own, nor did Salesforce notify Hanna about it – law enforcement did. How was the malware removed on November 11, 2019, without Defendants noticing it?

32. Hanna's customers' information was sold or is still for sale to criminals. This means that the breach was successful; unauthorized individuals accessed Hanna's customers' unencrypted, unredacted information, "including name, shipping address, billing address, payment card number, CVV code, and expiration date," and possibly more, without alerting Defendants, then offered the "scraped" information for sale online where the FBI or similar agency ran across it on or about December 5, 2020.

33. Around the same time the malware was supposedly removed from Salesforce's ecommerce platform, Hanna posted a job opening on LinkedIn for a "Director of Cyber Security," indicating that the company may not have had an adequate internal security lead that could monitor the website's systems or implement safeguards.[11] In the job description, Hanna's Director of Cyber Security would be "responsible for safeguarding all systems end points and network infrastructure from all forms of intrusion," and serving as a "primary point of contact concerning any cyber-attack activity and deal with any such incidents promptly and efficiently minimizing any reoccurrence."

34. During the time Hanna admits malware infected its Salesforce ecommerce platform and hackers were "scraping" customers' PII, and almost six weeks before Hanna "launched an investigation," the Portland, Oregon FBI office (located in the same city as

[11] *Hanna Andersson LinkedIn post for Director of Cyber Security*, November 2019, *available at*: https://www.linkedin.com/jobs/view/director-of-cyber-security-at-hanna-andersson-1518266875/ (last accessed January 28, 2020).

Defendant) issued a warning to companies about this exact type of fraud.

35. In the FBI's *Oregon FBI Tech Tuesday: Building a Digital Defense Against E-Skimming*, dated October 22, 2019, the agency stated:

> This warning is specifically targeted to . . . businesses . . . that take credit card payments online. E-skimming occurs when cyber criminals inject malicious code onto a website. The bad actor may have gained access via a phishing attack targeting your employees—or through a vulnerable third-party vendor attached to your company's server.[12]

36. The FBI gave some stern advice to companies like Hanna:

> Here's what businesses and agencies can do to protect themselves:
>
> - Update and patch all systems with the latest security software. Anti-virus and anti-malware need to be up-to-date and firewalls strong.
> - Change default login credentials on all systems.
> - Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.
> - Segregate and segment network systems to limit how easily cyber criminals can move from one to another.

37. But neither Salesforce nor Hanna apparently took this advice as hackers were actively scraping customers' PII off their website – until November 11, 2019 at the earliest.

38. Web scraping or skimming data breaches are commonly made possible through a vulnerability in a website or its backend content management system. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were collecting, causing customers' PII to be exposed for sale on the dark web.

Scraping and E-Skimming Breaches

39. *Magecart* is a loose affiliation of hacker groups responsible for skimming payment card attacks on various companies, including British Airways and Ticketmaster back in 2018.[13] 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

[12] Exhibit 2 (Oregon FBI Tech Tuesday_ Building a Digital Defense Against E-Skimming — FBI.pdf).

[13] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last accessed Jan. 30, 2020).

information to sell on the dark web.[14]

40. 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 Hanna admits the malware infecting Salesforce's platform scraped.

41. These cyber-attacks exploit weaknesses in the code of the ecommerce platform, without necessarily comprising the victim website's network or server.[15] These attacks have targeted third-party payment processors, like Salesforce, but the attack on British Airways in 2018 was far more tailored to the company's particular infrastructure.[16]

42. Magecart and these scraping breaches are not new: RiskIQ's earliest Magecart observation occurred on August 8th, 2010.[17] Thus, the Portland FBI's October 2019 warning was not the first time Defendants' would have been made aware of this type of breach – it's been going on for almost a decade and the well-publicized and widespread attacks on British Airways and Ticketmaster, among many others in and before 2018, should have alerted Defendants to the imminent danger facing Defendants' customers.

43. Unfortunately, despite all of the publicly available knowledge of the continued compromises of PII in this manner, Defendants' approach to maintaining the privacy and security of Plaintiffs' and Class members' PII was negligent, or at the very least, Defendants' did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect their customers' valuable PII.[18]

---

[14] *Id*.

[15] *What is Magecart and was it behind the Ticketmaster and BA hacks?*, Computerworld, Sep. 18, 2018, *available at*: https://www.computerworld.com/article/3427858/what-is-magecart-and-was-it-behind-the-ticketmaster-and-ba-hacks-.html (last accessed Jan. 30, 2020).

[16] *Id.*

[17] *Magecart: New Research Shows the State of a Growing Threat*, RiskIQ, Oct. 4, 2019, *available at*: https://www.riskiq.com/blog/external-threat-management/magecart-growing-threat/ (last accessed Jan. 30, 2020).

[18] While skimming attacks have become more popular, the practice of hackers using legitimate online services to host their infrastructure has expanded. Researchers at Malwarebytes recently discovered a rash of skimmers on the Heroku engagement platform, which is a PaaS run by Salesforce. This platform offers a free starter service for legitimate app developers to deploy, manage and scale their apps without needing to maintain their own infrastructure. Hackers are

Value of Personally Identifiable Information

44. 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.[19] 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.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

45. At all relevant times, Defendants 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.

46. Defendants were, or should have been, fully aware of the significant volume of daily credit and debit card transactions on its website – the malware infected Salesforce's platform during the lead up to Christmas 2019 – amounting to tens of thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

Plaintiff's Experience

47. Plaintiff Bernadette Barnes accessed www.hannaandersson.com from her home in Sacramento, California, on October 24, 2019, and purchased five items for a total of $119.59.

---

registering free accounts on Heroku to host their skimming schemes. Malwarebytes reported its findings to the Salesforce Abuse Operations team in late 2019. *There's an app for that: web skimmers found on PaaS Heroku*, Malwarebytes Labs, Dec. 4, 2019, available at: https://blog.malwarebytes.com/web-threats/2019/12/theres-an-app-for-that-web-skimmers-found-on-paas-heroku/ (last accessed Jan. 31, 2020).

[19] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 30, 2020).

[20] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 30, 2020).

[21] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Jan. 30, 2020).

48. Ms. Barnes made these purchases through her Hanna account. On the payment platform, Ms. Barnes entered her PII: name, billing and shipping addresses, payment card type and full number, CVV code, credit card expiration date, and email address. During this transaction, Ms. Barnes was never asked to "agree" to "Terms of Use."

49. At 8:37 pm on the same day, Hanna emailed confirmation of the purchases to Ms. Barnes, and the items were delivered 7-10 days later.

50. Ms. Barnes received the January 15, 2020 *Notice of Security Incident* from Hanna's President and CEO, Mike Edwards, on or about January 20, 2020. She did not receive the *Notice of Security Incident* sent by Hanna to Attorneys General.

51. As a result of the notice, Ms. Barnes spent time dealing with the consequences of the data breach, which includes time spent reviewing the account compromised by the breach, contacting her credit card company, exploring credit monitoring options, and self-monitoring her accounts.

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

53. Now, due to Defendants' misconduct and the resulting data breach, hackers obtained her PII at no compensation to Plaintiff whatsoever. That is money lost for Plaintiff, and money gained for the hackers, who could sell the PII for at least $15 on the dark web.

V. CLASS ALLEGATIONS

54. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 53.

55. Plaintiff brings this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class: **All individuals whose PII was compromised in the data breach announced by Hanna Andersson on January 15, 2020 (the "Nationwide Class").**

56. The California Class is initially defined as follows: **All persons residing in**

California whose PII was compromised in the data breach announced by Hanna Andersson on January 15, 2020 (the "California Class").

57. Excluded from the Class are the following individuals and/or entities: Defendants and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have 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.

58. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

59. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendants have identified thousands of customers whose PII may have been improperly accessed in the data breach, including approximately over 10,000 in California alone, and the Classes are apparently identifiable within Defendants' records.

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

a. Whether and when Defendants actually learned of the data breach and whether its response was adequate;

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

c. Whether Defendants breached that duty;

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

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class members' PII;

f. Whether Defendants knew or should have known that they did not employ

reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or misuse of that PII;

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

h. Whether Defendants caused Plaintiff and Class members damages;

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

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

k. Whether Defendants violated California's Deceptive and Unfair Trade Practices Act by failing to implement reasonable security procedures a practices; and

l. Whether Defendants violated California's California Consumer Privacy Act by failing to maintain reasonable security procedures and practices appropriate to the nature of the PII.

61. **Typicality**: Plaintiff's claims are typical of those of other Class members because all had their PII compromised as a result of the data breach, due to Defendants' misfeasance.

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

63. **Superiority and Manageability**: Under 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, Defendants' 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. The Terms of Service for Salesforce requires application of California law.

64. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have 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.

65. 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 Defendants owed a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

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

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants 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 Defendants' wrongful conduct.

COUNT I
(Negligence)
(On Behalf of Plaintiff and the Nationwide Class)

66. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 53.

67. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

68. The legal duties owed by Defendants to Plaintiff 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 Plaintiff and Class members in its possession;

b. To protect PII of Plaintiff 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 Plaintiff and Class members of the data breach.

69. In addition, Cal. Civ. Code §1798.81.5 requires Defendants to take reasonable steps and employ reasonable methods of safeguarding the PII of Class members who are California residents.

70. Defendants' 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), 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 Defendants.

71. Various FTC publications and data security breach orders further form the basis of Defendants' duty.[22] Plaintiff and Class members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

72. Defendants breached its duties to Plaintiff and Class members. Defendants 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 were surging in 2018 and on the rise in 2019, and the FBI issued its October 2019 warning right under Defendants' noses during the breach.

---

[22] *See, e.g., Data Protection: Actions taken by Equifax and Federal Agencies in Response to the 2017 Breach*, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (Aug. 30, 2019), *available at*: https://www.gao.gov/products/GAO-18-559 (regarding the Equifax data breach)(last accessed Jan. 30, 2020).

73. Defendants knew or should have known that its security practices did not adequately safeguard Plaintiff's and the other Class members' PII, including, but not limited to, the failure to detect the malware infecting Defendants' ecommerce platform from at least September 16 to November 11, 2019.

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

75. Defendants breached the duties it owes to Plaintiff 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.*, Hanna claims its website is PCI DSS compliant and uses SSL/TLS technology to encrypt customers' order information, such as name, address, and credit card number, during data transmission, but that did not occur here);

c. Failing to act despite knowing or having reason to know that Defendants' systems were vulnerable to E-skimming or similar attacks (*e.g.*, the steps Hanna is taking in response to this data breach "to re-secure the online purchasing platform . . . and to further harden it against compromise, including increasing use of multi-factor authentication and enhanced system monitoring" should have been taken beforehand); and

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

76. Due to Defendants' conduct, Plaintiff and Class members are entitled to credit monitoring. 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 Hanna's customers' names from the website, they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and credit card expiration dates. They got the *fullz* – everything they need to illegally use Hanna's 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.

77. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[23] Annual subscriptions for credit monitoring plans range from approximately $219 to $329 per year.

78. As a result of Defendants' negligence, Plaintiff 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 remains for sale on the dark web and is in Defendant's possession, subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers

[23] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring, but it only monitors victims' credit reports at one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

and former customers in their continued possession; (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 Plaintiff and Class members, including ongoing credit monitoring.

79. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' negligent conduct.

COUNT II
(Declaratory Judgment)
(On Behalf of Plaintiffs and the Nationwide Class)

80. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 53.

81. Defendants owe duties of care to Plaintiff and Class members which would require it to adequately secure PII.

82. Defendants still possess PII regarding Plaintiff and Class members.

83. Plaintiff and Class members' PII is still for sale on the dark web.

84. Although Defendants claim they have "taken steps to re-secure the online purchasing platform on its website and to further harden it against compromise, including increasing use of multi-factor authentication and enhanced system monitoring," there is no detail on what, if any, fixes have really occurred.

85. Plaintiff and Class members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

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

87. Plaintiff, therefore, seeks a declaration that (1) each 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, Defendants must implement and maintain reasonable security measures, including, but not limited to:

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

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendants user applications be segmented by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants conduct regular database scanning and securing checks;

f. Ordering that Defendants routinely and continually conduct 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. Ordering Defendants to purchase credit monitoring services for Plaintiff and Class members for a period of ten years; and

h. Ordering Defendants to meaningfully educate its users about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendants customers must take to protect themselves.

//
//
//
//
//

COUNT III
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §17200 – Unlawful Business Practices
(On Behalf of Plaintiffs and the Nationwide Class, Or In The Alternative, On Behalf of the California Class)

88. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 53.

89. Defendants have violated Cal. Bus. and 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 California Class.

90. 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 Plaintiffs' and California Class members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Class members' PII 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 PII of Plaintiff and the California Class members.

91. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the data breach to California Class members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendant Salesforce has still not provided such information to Plaintiff and the California Class members.

92. As a direct and proximate result of Defendants unlawful practices and acts, Plaintiff and the California 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 California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

93. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard California Class members' PII 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 members of the California Class.

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

COUNT IV
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §17200 – Unfair Business Practices
(On Behalf of Plaintiffs and the Nationwide Class,
Or In The Alternative, On Behalf of the California Class)

95. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 53.

96. Defendants engaged in unfair acts and practices with respect to the hotel services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Class members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and California Class members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Class members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the California Class members outweighed their utility, if any.

97. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect California Class members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff

and California Class members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the California Class members outweighed their utility, if any.

98. As a direct and proximate result of Defendants' acts of unfair practices and acts, Plaintiff and the California 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 California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

99. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard California Class members' PII 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 members of the California Class.

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

101. Plaintiff and the California Class members reserve the right to amend this Complaint as of right to seek damages and relief under Cal. Civ. Code § 1798.100, *et seq*.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class members, requests judgment against the Defendants and that the Court grant the following:

A. An order certifying the Nationwide Class and California Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class

members' PII;

C. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;

D. An award of compensatory, statutory, and punitive damages, in an amount to be determined;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: February 3, 2020

Respectfully Submitted,

By: /s/ M. Anderson Berry

M. Anderson Berry
aberry@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

John A. Yanchunis (*Pro Hac Vice* Forthcoming)
jyanchunis@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402 (fax)