RACHELE R. BYRD (190634)
byrd@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

MATTHEW M. GUINEY (*pro hac vice forthcoming*)
guiney@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
270 Madison Avenue
New York, NY 10016
Telephone: 212/545-4600
Facsimile: 212/545-4677

Attorneys for Plaintiffs

[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

KRISTA GILL and DOUG SUMERFIELD, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

HANNA ANDERSSON, LLC and SALESFORCE.COM, INC.

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Krista Gill ("Gill") and Doug Sumerfield ("Sumerfield") (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals, hereby allege upon personal knowledge of the facts respectively pertaining to their own actions, and upon information and belief as to all other matters, by and through their undersigned counsel, and bring this Class Action Complaint against defendants Hanna Andersson, LLC ("Hanna Andersson") and Salesforce.com, Inc. ("Salesforce" and, collectively, "Defendants").

NATURE OF ACTION

1. Plaintiffs assert this class action against Defendants for their failure to exercise reasonable care in securing and safeguarding their customers' sensitive personal information ("SPI"), including customer names, payment card numbers, payment card expiration dates, and payment card security codes.

2. On January 15, 2020, Hanna Andersson sent letters to customers and states attorneys general stating that it "had obtained evidence that an unauthorized third party had accessed information entered on Hanna Andersson's website concerning purchases made between September 16 and November 11, 2019" (the "Data Breach").[1] Attempting to avoid the spotlight, Hanna Andersson sent this letter directly to customers and state law enforcement without making a public press release. News soon got out, however.

3. This type of customer payment data breach, called a Magecart attack, was simply the most recent in a long line of similar attacks on e-commerce platforms. The Hanna Andersson attack was no less than the second successful recent Magecart attack upon a platform that was part of Salesforce's Commerce Cloud Unit, its commercial hosting service.[2]

4. More broadly, Magecart attacks on online platforms have become very popular in the past few years. For example, Salesforce customer Macy's faced a similar Magecart attack

---

[1] https://www.documentcloud.org/documents/6662592-Hanna-Andersson-Notice-of-Data-Breach-to-Consumers.html (last visited Mar. 2, 2020).

[2] *See US Retailer Hanna Andersson Hacked to Steal Credit Cards*, BLEEPING COMPUTER, https://www.bleepingcomputer.com/news/security/us-retailer-hanna-andersson-hacked-to-steal-credit-cards/ (last visited Mar. 2, 2020).

last October where hackers successfully stole payment card information from its website for a week.[3]

5. Defendants could have prevented this Data Breach. Magecart attacks on e-ecommerce platforms are among the most popular types of attacks by hackers today. While many retailers, restaurant chains, and other companies have responded to data breaches by adopting technology that helps make transactions more secure, Defendants did not.

6. The Data Breach was the result of Defendants' inadequate approach to data security and protection of SPI that it collected during the course of its business. The deficiencies in Defendants' data security were so significant that the malware installed by hackers remained undetected and intact in Defendants' systems for approximately two months.

7. Defendants disregarded the rights of Plaintiffs and the Class by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard SPI, failing to take available steps to prevent the Data Breach, failing to monitor and timely detect the Data Breach, and failing to provide Plaintiffs and the Class prompt and accurate notice of the Data Breach.

8. As a result of Defendants' Data Breach, Plaintiffs' and Class members' SPI has been exposed to criminals for misuse and have, in fact, been misused. The injuries Plaintiffs and the Class suffered as a direct result of the Data Breach include:

a. unauthorized charges on debit and credit card accounts;

b. theft of personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;

---

[3] *Macy's Hit by Magecart Card-Skimming Attack*, CISO MAG (Nov. 20, 2019), https://www.cisomag.com/macys-hit-by-magecart-card-skimming-attack/; *see also Macy's moves its mission-critical commerce app to Heroku*, SALESFORCE, https://www.salesforce.com/products/platform/app-gallery/macys/ (last visited Mar. 3, 2020).

d. damages arising from the inability to use debit or credit card accounts because accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach, including but not limited to foregoing cash back rewards;

e. damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the Data Breach, including, but not limited to, missed bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit;

f. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, lost productivity and opportunity(ies), time taken from the enjoyment of one's life, and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by SPI being exposed for theft and sale on the dark web;

h. costs of products purchased at Defendants' website during the period of the Data Breach because Plaintiffs and the Class would not have purchased products from Defendants' website had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard SPI;

i. damages to and diminution in value of SPI entrusted to Defendants for the sole purpose of purchasing products and services from Defendants; and

j. the loss of Plaintiffs' and Class members' privacy.

9. The injuries Plaintiffs and the Class suffered were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for SPI.

10. Plaintiffs and the Class retain a significant interest in ensuring that their SPI, which remains in Defendants' possession, is protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated consumers whose SPI was stolen.

11. Plaintiffs, individually and on behalf of similarly situated consumers, seek to recover damages, equitable relief, including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

PARTIES

12. Plaintiffs Krista Gill and Doug Sumerfield are natural persons and a married couple residing in Alexandria, Virginia.

13. Defendant Hanna Andersson, LLC is a Delaware corporation with its principal place of business at 608 NE 19th Ave., Portland, Oregon 97232. It is wholly-owned by L Catterton, a private equity company.

14. Defendant Salesforce.com, Inc. is a Delaware corporation with its principal place of business at 415 Mission St., San Francisco, California 94105.

JURISDICTION AND VENUE

15. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties to this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class.[4]

16. This Court has personal jurisdiction over Defendant Salesforce because its principal place of business is in the Northern District of California and Salesforce is authorized to and regularly conducts business in the Northern District of California.

[4] A letter sent to the North Dakota Attorney General by counsel for Hanna Andersson noted that there were 374 residents of North Dakota alone affected by the Data Breach.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.