IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

JUSTIN AHN, KEVIN BERSCH, LEIGHTON BLACKWOOD and KRISTIN WALKER, individually, and on behalf of all others similarly situated, Plaintiffs, v. HERFF JONES, LLC, Defendant.	Case No.: 1:21-cv-1381 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Justin Ahn, Kevin Bersch, Leighton Blackwood and Kristin Walker ("Plaintiffs") bring this Class Action Complaint against Defendant Herff Jones, LLC. ("Herff Jones" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Herff Jones sells and rents products related to school graduation, including caps, gowns, class rings, and graduation announcements.

2. Beginning at least as early as May 5, 2021, graduating college seniors on Reddit began reporting that they had incurred fraudulent credit and debit card charges as a result of renting graduation caps and gowns from Defendant. These rentals were the only common charges that all students had in common.

3. Beginning on or around May 11, 2021, news organizations began reporting that

Defendant had suffered a breach (the "Data Breach") of customers' personally identifiable information ("PII") and that numerous students were reporting that they had incurred fraudulent charges and that some had had their accounts frozen as a result of the Data Breach.

4. As of this writing, students at The University of Houston, Purdue University, The University of Illinois and Urbana-Champaign, The State University of New York at Binghamton and many other schools had reported their PII stolen as part of the Data Breach.

5. Not only did hackers skim Herff Jones' customers' PII, on information and belief, the stolen names and payment card information are now for sale on the dark web. That means the Data Breach worked. Hackers accessed and then offered for sale the unencrypted, unredacted, stolen PII to criminals. Because of Defendant's Data Breach, customers' PII is still available on the dark web for criminals to access and abuse. Herff Jones' customers face a lifetime risk of identity theft.

6. All of this personally identifiable information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect customers' data.

7. On May 12, 2021, Herff Jones confirmed the data breach, though as yet has provided no details. On information and belief, the number of affected customers appears to be at least in the thousands.

8. 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 Defendant's websites and ecommerce platforms for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

9. Plaintiffs and similarly situated Herff Jones customers ("Class Members") have

suffered injury as a result of Defendant's conduct. These injuries 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 New York's General Business Law; and (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 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.

PARTIES

10. Plaintiff Justin Ahn is a citizen of New York residing in Tompkins County, New York. Mr. Ahn used Defendant's website on April 13, 2021 to rent a cap and gown for his graduation ceremony, using his debit card issued by J.P. Morgan Chase. On May 13, 2021, he discovered a fraudulent charge on his bank account which was the result of the data breach.

11. Plaintiff Kevin Bersch is a citizen of New Jersey residing in Tippecanoe County, Indiana. Mr. Bersch used Defendant's website on March 27, 2021 to rent a cap and gown for his graduation ceremony, using his credit card issued by TD Bank. On May 24, 2021, he discovered $396.49 in fraudulent charges on his bank account which were the result of the data breach. As of the filing of this complaint, those charges have not been reversed or refunded by the bank.

12. Plaintiff Leighton Blackwood is a citizen of New York residing in Broome County, New York. Mr. Blackwood used Defendant's website on April 15, 2021 to rent a cap and gown for his graduation ceremony, using his debit card issued by M&T Bank. On May 13, 2021, he discovered $255.31 in fraudulent charges on his bank account which were the result of the data

breach. As of the filing of this complaint, those charges have not been fully reversed or refunded by the bank.

13. Plaintiff Kristin Walker is a citizen of California residing in Los Angeles County, California. Ms. Walker used Defendant's website on March 31, 2021 to rent a cap and gown for her graduation ceremony, using her debit card issued by Bank of America. On May 5th 2021, she discovered $229.91 in fraudulent charges on her bank account which were the result of the data breach.

14. Defendant Herff Jones, LLC. is an Indiana corporation with its principle place of business at 4625 W. 62nd Street, Indianapolis, Indiana, 46268. Herff Jones advertises and rents or sells goods to customers nationwide through its website as well as through contracted representatives.

15. Since 2014, Herff Jones has been a wholly owned subsidiary of Varsity Brands, Inc.

JURISDICTION AND VENUE

16. 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 in 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.

17. 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. A substantial part of the events giving rise to the claims alleged herein occurred within this judicial district. Further, Defendant conducts business regularly throughout this District, as is evidenced by its agreements with Purdue University for the licensing, sale, and

rental of graduate regalia specific to both schools and its rental and sales agreements with students and former students at both schools.

FACTUAL ALLEGATIONS

Background

18. Herff Jones was founded in 1920 as a manufacturer of collegiate insignia and class rings.

19. Today Herff Jones rents and/or sells graduation attire, class rings, announcements, and other products generally related to high school, college, or post-baccalaureate graduation.

20. Schools contract directly with Herff Jones for rental and sales of regalia in connection with graduations – students do not individually pick their preferred regalia vendor at graduation time.

21. Students generally do not have the freedom to choose a preferred regalia vendor. Their choice is limited to their school's choice.

22. Customers purchasing online demand security to safeguard their PII.

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.

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.[1]

[1] PCI Security Standards Council, https://www.pcisecuritystandards.org/ (last accessed May 24, 2021).

25. To rent or purchase products on Herff Jones' website for recent and/or upcoming graduates[2], customers generally do so without creating a dedicated account. To complete a purchase, at a minimum, the customer must enter the following PII:

- Name;
- billing address;
- delivery address;
- email address;
- telephone number;
- 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).

26. At no time during the final checkout process does Herff Jones require customers to expressly agree to "Terms of Use," "Terms of Service" or "Terms & Conditions."

The Data Breach

27. Beginning on or about May 5, 2021, students on Reddit and other websites and social media sites began noticing a common pattern of stolen payment card data. The only source that these students all appeared to have in common was Herff Jones, their school's regalia vendor.[3]

28. Since the initial postings, students at The University of Houston, Purdue University,

[2] https://collegegrad.herffjones.com

[3] *See, e.g.,* https://www.reddit.com/r/Purdue/comments/n56ga5/graduating_seniors_look_here_herff_jones_data/?utm_source=share&utm_medium=ios_app&utm_name=iossmf and https://www.reddit.com/r/UniversityOfHouston/comments/n8w049/herff_jones_data_breach/ (last accessed May 24, 2021).

Towson University, The University of Southern California, The University of Wisconsin at Madison, Cornell University, Boston University, The University of Illinois at Urbana-Champaign, The University of California at Davis, The State University of New York at Binghamton, and others have complained of incurring fraudulent charges as a result of the breach.

29. On or around May 11, 2021, various news organizations began picking up on the Data Breach, noting that Herff Jones has admitted that "some information had been stolen."[4]

30. Herff Jones' customers' information is likely for sale on the dark web and, on information and belief, is still for sale to criminals. This means that the Data Breach was successful; unauthorized individuals accessed Herff Jones' customers' unencrypted, unredacted information, including "Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Payment Card Number; Payment Card Security Code; and Payment Card Month/Year of Expiration," and possibly more, without alerting Defendant, then offered the "scraped" information for sale online. There is no indication that Defendant's customers' PII was removed from the dark web where it likely remains.

31. As of May 12, 2021, Herff Jones has posted an update on their website, which states, in its entirety, as follows:

> Herff Jones recently became aware of suspicious activity involving certain customers' payment card information. We promptly launched an investigation and engaged a leading cybersecurity firm to assist in assessing the scope of the incident. We have taken steps to mitigate the potential impact and notified law enforcement. Herff Jones is committed to the privacy and security of its customers and we take this responsibility seriously.
>
> During the course of our investigation, which is ongoing, we identified theft of certain customers' payment information.
>
> We sincerely apologize to those impacted by this incident. We are working diligently to identify and notify impacted customers. In the meantime, we have a

[4] https://www.fox61.com/article/news/nation-world/herff-jones-cap-gown-graduation-payment-information-theft/507-def01040-b9b9-40da-b0a0-50dc6733806f (last accessed May 24, 2021).

> dedicated customer service team that can be reached by calling 855-535-1795 between 9 a.m. and 9 p.m. EDT Monday through Friday.

32. As of this writing, Herff Jones has not yet provided notice to state attorneys general, to the public via press release, or to customers and lesees via email or physical mail, leaving many customers in the dark as to the vulnerability of their data.

33. Recently, the FBI issued yet another warning to companies about this exact type of fraud. 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.

34. The FBI gave some stern advice to companies like Herff Jones:

> 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.

35. But Defendant apparently did not take this advice: hackers scraped customers' PII off its website—and continued to do so until at least May 2021.

36. Web scraping or skimming data breaches are commonly made possible through a

vulnerability in a website or its backend content management system. Defendant 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 and sold on the dark web.

Scraping and E-Skimming Breaches

37. *Magecart* is a loose affiliation of hacker groups responsible for skimming payment card attacks on various companies, including British Airways and Ticketmaster.[5] 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.[6]

38. 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 appears to have been scraped from Herff Jones' ecommerce platform.

39. These cyber-attacks exploit weaknesses in the code of the ecommerce platform, without necessarily compromising the victim website's network or server. These attacks often target third-party payment processors like Shopify and Salesforce.

40. 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 Plaintiff's 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 its customers' valuable PII.

---

[5] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost (Aug. 28, 2019), https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last accessed May 24, 2021).

[6] *Id*.

Value of Personally Identifiable Information

41. 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.[7] 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.[8] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[9]

42. 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.

43. Defendant were, or should have been, fully aware of the significant volume of daily credit and debit card transactions on its website, amounting to thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

Plaintiff Ahn's Experience

44. Plaintiff Justin Ahn placed an order to rent his cap and gown on or about April 13, 2021. He checked out used his J.P. Morgan Chase credit card.

45. On the payment platform, Mr. Ahn entered his PII: name, billing address, delivery

---

[7] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed May 24, 2021).

[8] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 24, 2021).

[9] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 24, 2021).

address, payment card type and full number, CVV security code, payment card expiration date, and email address. During this transaction, Mr. Ahn was not asked to "agree" to any "Terms of Service" or to review the "Privacy Policy."

46. On or about May 13, 2021, an unauthorized charge was made on Mr. Ahn's credit card.

47. J. P. Morgan Chase changed the account number in response to the illegal charges and mailed him a new card, which he has not yet received. Mr. Ahn had to take time out of his day during final examinations to deal with the fraudulent charges and the account number change. This was time he otherwise would have spent performing other activities, such as his job and/or leisure activities for the enjoyment of life. He also had to use alternative methods of payment until he received their new credit card.

48. As of the filing of this complaint, Mr. Ahn has not received direct notice from Defendant of the Data Breach.

49. Knowing that a hacker stole his PII, and that his PII may be available for sale on the dark web, has caused Mr. Ahn great concern. He is now very concerned about credit card theft and identity theft in general. This breach has given Mr. Ahn hesitation about using Herff Jones' services, and reservations about shopping on other online websites.

50. Now, due to Defendant's misconduct and the resulting Data Breach, hackers obtained his PII at no compensation to Mr. Ahn whatsoever. That is money lost for him, and money gained for the hackers – who could sell his PII on the dark web.

51. Mr. Ahn also suffered actual injury and damages in paying money to, and purchasing and/or renting products from, Defendant's website during the Data Breach, expenditures which he would not have made had Defendant disclosed that it lacked computer

systems and data security practices adequate to safeguard customers' PII from theft.

52. Moreover, Mr. Ahn suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

53. Plaintiff Justin Ahn has a continuing interest in ensuring his PII, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Justin Ahn's Efforts to Secure PII

54. Defendant's Data Breach caused Mr. Ahn harm.

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

56. Additionally, Mr. Ahn never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

57. Mr. Ahn stores any and all electronic documents containing his PII in a safe and secure location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card.

Plaintiff Bersch's Experience

58. Plaintiff Kevin Bersch placed an order to rent his cap and gown on or about March 27, 2021. He checked out used his TD bank credit card.

59. On the payment platform, Mr. Bersch entered his PII: name, billing address, delivery address, payment card type and full number, CVV security code, payment card expiration

date, and email address. During this transaction, Mr. Bersch was not asked to "agree" to any "Terms of Service" or to review the "Privacy Policy."

60. From May 5, 2021 to May 20, 2021, a series of 12 unauthorized purchases totaling $396.49 were made on the card.

61. Mr. Bersch contacted TD bank and they changed the account number in response to the illegal charges and mailed him a new card. Mr. Bersch had to take time out of his day to deal with the fraudulent charges and the account number change, as well as to change over recurring charges that would otherwise be made on the card. This was time he otherwise would have spent performing other activities, such as his job and/or leisure activities for the enjoyment of life. He also had to use alternative methods of payment until he received the new credit card.

62. As of the filing of this complaint, Mr. Bersch has not been reimbursed his fraudulent charges, and he has not received direct notice from Defendant of the Data Breach.

63. Knowing that a hacker stole his PII, and that his PII may be available for sale on the dark web, has caused Mr. Bersch great concern. He is now very concerned about credit card theft and identity theft in general. This breach has given Mr. Bersch hesitation about using Herff Jones' services, and reservations about shopping on other online websites.

64. Now, due to Defendant's misconduct and the resulting Data Breach, hackers obtained his PII at no compensation to Mr. Bersch whatsoever. That is money lost for him, and money gained for the hackers – who could sell his PII on the dark web.

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

66. Moreover, Mr. Bersch suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

67. Plaintiff Kevin Bersch has a continuing interest in ensuring his PII, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Kevin Bersch's Efforts to Secure PII

68. Defendant's Data Breach caused Mr. Bersch harm.

69. Prior to the activity described above during the period in which the Data Breach occurred, the debit card that Mr. Bersch used to purchase and/or rent products on Defendant's website had never been stolen or compromised. Mr. Blackwood regularly reviewed his credit reports and other financial statements routinely and to his knowledge this card had not been compromised in any manner.

70. Additionally, Mr. Bersch never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

71. Mr. Bersch stores any and all electronic documents containing his PII in a safe and secure location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card.

Plaintiff Blackwood's Experience

72. Plaintiff Leighton Blackwood placed an order to rent his cap and gown on or about April 15, 2021. He checked out used his debit card, issued by M&T Bank.

73. On the payment platform, Mr. Blackwood entered his PII: name, billing address, delivery address, payment card type and full number, CVV security code, payment card expiration date, and email address. During this transaction, Mr. Blackwood was not asked to "agree" to any

"Terms of Service" or to review the "Privacy Policy."

74. May 11, 2021, a series of two unauthorized purchases totaling $255.31 were made on the card.

75. M&T Bank changed the account number in response to the illegal charges and mailed him a new card. Mr. Blackwood had to take time out of his day to deal with the fraudulent charges and the account number change, as well as to change over recurring charges that would otherwise be made on the card. This was time he otherwise would have spent performing other activities, such as his job and/or leisure activities for the enjoyment of life. He also had to use alternative methods of payment until he received their new credit card.

76. As of the filing of this complaint, Mr. Blackwood has not been fully reimbursed his fraudulent charges, and he has not received direct notice from Defendant of the Data Breach.

77. Knowing that a hacker stole his PII, and that his PII may be available for sale on the dark web, has caused Mr. Blackwood great concern. He is now very concerned about credit card theft and identity theft in general. This breach has given Mr. Blackwood hesitation about using Herff Jones' services, and reservations about shopping on other online websites.

78. Now, due to Defendant's misconduct and the resulting Data Breach, hackers obtained his PII at no compensation to Mr. Blackwood whatsoever. That is money lost for him, and money gained for the hackers – who could sell his PII on the dark web.

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

80. Moreover, Mr. Blackwood suffered imminent and impending injury arising from

the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

81. Plaintiff Leighton Blackwood has a continuing interest in ensuring his PII, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Leighton Blackwood's Efforts to Secure PII

82. Defendant's Data Breach caused Mr. Blackwood harm.

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

84. Additionally, Mr. Blackwood never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

85. Mr. Blackwood stores any and all electronic documents containing his PII in a safe and secure location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card.

Plaintiff Walker's Experience

86. Plaintiff Kristin Walker placed an order to rent her cap and gown on or about March 31, 2021. She checked out used her Bank of America debit card.

87. On the payment platform, Ms. Walker entered her PII: name, billing address, delivery address, payment card type and full number, CVV security code, payment card expiration date, and email address. During this transaction, Mr. Blackwood was not asked to "agree" to any

"Terms of Service" or to review the "Privacy Policy."

88. From May 5, 2021 to May 6, 2021, a series of six unauthorized purchases totaling $229.91were made on the card.

89. Bank of America changed the account number in response to the illegal charges and mailed him a new card. Ms. Walker had to take time out of her day to deal with the fraudulent charges and the account number change, as well as to change over recurring charges that would otherwise be made on the card. This was time she otherwise would have spent performing other activities, such as her job and/or leisure activities for the enjoyment of life. He also had to use alternative methods of payment until he received their new credit card.

90. Ms. Walker was ultimately refunded her fraudulent charges on or about May 10, 2021, but did not have access to those funds during that time.

91. Ms. Walker has not received direct notice from Defendant of the Data Breach.

92. Knowing that a hacker stole her PII, and that her PII may be available for sale on the dark web, has caused Ms. Walker great concern. She is now very concerned about credit card theft and identity theft in general. This breach has given Ms. Walker hesitation about using Herff Jones' services, and reservations about shopping on other online websites.

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

94. Ms. Walker also suffered actual injury and damages in paying money to, and purchasing and/or renting 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.

95. Moreover, Ms. Walker 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.

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

Plaintiff Kristin Walker's Efforts to Secure PII

97. Defendant's Data Breach caused Ms. Walker harm.

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

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

100. Ms. Walker stores any and all electronic documents containing her PII in a safe and secure location, and destroys any documents he receives in the mail that contain any of her PII, or that may contain any information that could otherwise be used to compromise her credit card.

CLASS ALLEGATIONS

101. 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 that is the subject of this complaint (the "Nationwide Class").

102. The California Subclass is defined as follows:

All persons residing in California whose PII was compromised in the data breach that is the subject of this complaint (the "California Subclass").

103. The Indiana Subclass is defined as follows:

All persons residing in Indiana whose PII was compromised in the data breach that is the subject of this complaint (the "Indiana Subclass").

104. The New York Subclass is defined as follows:

All persons residing in New York whose PII was compromised in the data breach that is the subject of this complaint (the "New York Subclass").

105. Excluded from the Class 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 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 Defendant's 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 Defendant's immediate family members.

106. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

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

108. **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 they 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 New York's General Business Law (N.Y.G.B.L. §§ 349, *et seq*.);

l. Whether Defendant violated California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq*.); and

m. Whether Defendant violated California's Consumer Legal Remedies Act (Cal. Civ. Code §§ 1770, *et seq*.).

109. **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.

110. **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.

111. **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.

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

113. 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 their 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 Nationwide Class)

114. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

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

116. 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.

117. 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), 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.

118. 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.

119. Defendant breached its 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.

120. Defendant knew or should have known that its 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 ecommerce platform for months.

121. 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.

122. Defendant breached the duties they owe 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 ecommerce 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 ecommerce platform, nor did they 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.

123. Due to Defendant's conduct, Plaintiffs 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 Herff Jones's customers' names from the website, but they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and payment card expiration dates. They got the *fullz*—everything they need to illegally use Herff Jones' 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.

124. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[10] Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

125. 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 fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (v) future costs in terms of time, effort, and money that will be

[10] 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.

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.

SECOND CLAIM FOR RELIEF

Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

126. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

127. When Plaintiffs and Class Members provided their PII to Defendant in exchange for Defendant's products, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their PII.

128. Defendant solicited and invited Plaintiffs and Class Members to provide their PII as part of Defendant's regular business practices and as essential to the sales transaction process for card payment transactions. This conduct thus created implied contracts between Plaintiffs and Class Members on one hand, and Defendant on the other hand. Plaintiffs and Class Members accepted Defendant's offer by providing their PII to Defendant in connection with their purchases from Defendant.

129. When entering into these implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

130. Defendant's implied promise to safeguard Plaintiffs' and Class Members' PII is evidenced by a duty to protect and safeguard PII that Defendant required Plaintiffs and Class Members to provide as a condition of entering into consumer transactions with Defendant.

131. Plaintiffs and Class Members paid money to Defendant to purchase products or services from Defendant. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

132. Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from customers' continued use of Defendant's website—that Defendant would adequately safeguard PII. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiffs and Class Members.

133. Plaintiffs and Class Members value data security and would not have provided their PII to Defendant in the absence of Defendant's implied promise to keep the PII reasonably secure.

134. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

135. Defendant breached their implied contracts with Plaintiffs and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

136. As a direct and proximate result of Defendant's breach of the implied contract, Plaintiffs and Class Members sustained damages as alleged herein.

137. Plaintiffs and Nationwide Class members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

138. Plaintiffs and Nationwide Class Members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

THIRD CLAIM FOR RELIEF

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

139. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

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

141. Defendant still possesses PII regarding Plaintiffs and Class Members.

142. Although Herff Jones claims in its *Cyber Security Incident Update* that it has "taken steps to mitigate the potential impact," there is no detail on what, if any, fixes have occurred.

143. 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.

144. 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.

145. Plaintiffs, therefore, seek a declaration that (1) each of 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.

FOURTH CLAIM FOR RELIEF

Violation of New York General Business Law §§ 349, *et seq*.
(On Behalf of Plaintiffs Ahn and Blackwood and the Nationwide Class, or, in the alternative, On Behalf of Plaintiffs Ahn and Blackwood and the New York Subclass)

146. Plaintiffs Ahn and Blackwood re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

147. New York's General Business Law § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce.

148. In its provision of services throughout the State of New York, Defendant conducts business and trade within the meaning and intendment of New York's General Business Law § 349.

149. Plaintiffs Ahn and Blackwood and members of the New York Subclass are consumers who conducted transactions with Defendant for their personal use.

150. By the acts and conduct alleged herein, Defendant has engaged in deceptive, unfair, and misleading acts and practices, which include, without limitation, the expectation that Defendant would implement adequate cybersecurity, when in fact Defendant did not.

151. The foregoing deceptive acts and practices were directed at consumers.

152. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the ability and measures taken by Defendant to safeguard consumer PII, and to induce consumers to enter transactions with Defendant.

153. By reason of this conduct, Defendant engaged in deceptive conduct in violation of GBL § 349.

154. Defendant's actions are the direct, foreseeable, and proximate cause of the damages that Plaintiffs Ahn and Blackwood and Members of the Classes have sustained from having provided their PII to Defendant, which was exposed in the data breach.

155. As a result of Defendant's violations, Plaintiffs Ahn and Blackwood and Members of the Classes have suffered damages because: (a) they would not have provided their PII to Defendant had they known Defendant did not use "reasonable security measures, including physical, administrative, and technical safeguards to help us protect your information from unauthorized access, use and disclosure"; (b) they have suffered identity theft and/or fraudulent charges and their PII has been devalued as a result of being exposed in the data breach; and (c) Plaintiff and Members of the Classes must spend considerable time and expenses dealing with the effects of the data breach, and are now at greater risk for future harm stemming from the data breach.

156. On behalf of themselves and other Members of the Classes, Plaintiffs Ahn and Blackwood seek to recover their actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

FIFTH CLAIM FOR RELIEF

Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.*—Unlawful Business Practices
(On Behalf of Plaintiff Kristin Walker and the California Subclass)

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

158. Defendant has 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 Subclass.

159. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Subclass Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and the California Subclass Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiff and the California Subclass Members.

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

161. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

162. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Walker's and California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Defendant's 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 Subclass.

163. Plaintiff Walker and California Subclass Members seek relief under Cal. Bus. & Prof. Code §§ 17200, *et seq.*, including, but not limited to, restitution to Plaintiff Walker and California Subclass Members of money or property that Defendant may have acquired by means of their unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant 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.

SIXTH CLAIM FOR RELIEF

Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq*.—Unfair Business Practices
(On Behalf of Plaintiff Kristin Walker and the California Subclass)

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

165. Defendant engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and the California Subclass Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's California Subclass 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 Subclass 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 Subclass Members outweighed their utility, if any.

166. Defendant 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 Subclass 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 Subclass 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 Subclass Members outweighed their utility, if any.

167. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff Walker and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

168. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Nationwide and California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Defendant's 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 Subclass.

169. Plaintiff Walker and California Subclass Members seek relief under Cal. Bus. & Prof. Code §§ 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the California Subclass Members of money or property that the Defendant may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to

Defendant 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.

SEVENTH CLAIM FOR RELIEF

Violation of the California Consumer Privacy Act,
Cal. Civ. Code §§ 1798.100, *et seq*.
(On Behalf of Plaintiff Kristin Walker and the California Subclass)

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

171. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Walker's and California Subclass Members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Walker and California Subclass Members.

172. As a direct and proximate result of Defendant's acts, Plaintiff Walker's and the California Subclass Members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer systems and/or from the dark web, where hackers further disclosed Defendant's customers' PII.

173. As a direct and proximate result of Defendant's acts, Plaintiff Walker and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

174. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff Walker and the California Subclass Members.

175. Defendant collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

176. At this time, Plaintiff Walker and California Subclass Members seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

177. On May 21, 2021, Plaintiff Walker mailed Herff Jones notice in writing, via U.S. certified mail, notice which identified the specific provisions of this title she alleges Herff Jones has violated. If within 30 days of Plaintiff Walker's written notice Defendant fails to "actually cure" its violation of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiff Walker will amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

EIGHTH CLAIM FOR RELIEF

Violation of California's Consumers Legal Remedies Act,
Cal. Civ. Code §§ 1750, *et seq*.
(On Behalf of Plaintiff Kristin Walker and the California Subclass)

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

179. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Defendant's acts, omissions, representations and practices as described herein fall within the CLRA because the design, development, and marketing of Defendant's products are intended to and did result in sales and rental of consumer products.

180. Plaintiff Walker and the other California Subclass Members are consumers within the meaning of Cal. Civ. Code § 1761(d).

181. Defendant's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By omitting key information about the safety and security of its network Defendant violated the CLRA. Defendant had exclusive knowledge of undisclosed material facts, namely, that its network was defective and/or unsecure, and withheld that knowledge from California Subclass Members.

182. Defendant's acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of section 1770 the CLRA, which provides, in relevant part, that:

a. The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:

(5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . .

> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (9) Advertising goods or services with intent not to sell them as advertised.
>
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
>
> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

For purposes of the CLRA, omissions are actionable along with representations.

183. Defendant knew or should have known that it did not employ reasonable measures that would have kept California Subclass Members' PII secure and prevented the loss or misuse of their PII. For example, Defendant failed to take reasonable steps to prevent the loss of PII through their servers through appropriate encryption and industry best practices.

184. Defendant's deceptive acts and business practices induced California Subclass Members to provide PII, including payment card information, for the purchase or rental of Defendant's products. But for these deceptive acts and business practices, California Subclass Members would not have purchased or rented Defendant's products, or would not have paid the prices they paid for those products.

185. Defendant's representations that it would secure and protect California Subclass Members' PII in its possession were facts that reasonable persons could be expected to rely upon when deciding whether to purchase insurance services.

186. California Subclass Members were harmed as the result of Defendant's violations of the CLRA, because their PII was compromised, placing them at a greater risk of identity theft; they lost the unencumbered use of their PII; and their PII was disclosed to third parties without their consent.

187. California Subclass Members suffered injury in fact and lost money or property as the result of Defendant's failure to secure its PII; the value of their PII was diminished as the result of Defendant's failure to secure their PII; and they have expended time and money to rectify or guard against further misuse of their PII.

188. Defendant's conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby justifying an award of punitive damages.

189. As the result of Defendant's violation of the CLRA, Plaintiff Walker, on behalf of herself, California Subclass Members, and the general public of the State of California, seek injunctive relief prohibiting Defendant from continuing these unlawful practices pursuant to California Civil Code § 1782(a)(2), and such other equitable relief, including restitution, and a declaration that Defendant's conduct violated the CLRA.

190. Pursuant to Cal. Civ. Code § 1782, on May 21, 2021, Plaintiff Walker mailed Herff Jones notice in writing, via U.S. certified mail, of the particular violations of Cal. Civ. Code § 1770 of the CLRA and demanded that they rectify the actions described above by providing complete monetary relief, agreeing to be bound by Herff Jones' legal obligations and to give notice to all affected customers of their intent to do so. If Defendant fails to respond to the letter within 30 days and to take the actions demanded to rectify their violations of the CLRA, Plaintiff Walker will amend this Complaint to seek damages and attorneys' fees as allowed by the CLRA.

NINTH CLAIM FOR RELIEF

Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

191. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

192. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of monies paid for goods available on Defendant's websites.

193. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. Defendant also benefited from the receipt of Plaintiffs' and Class Members' PII, as this was used by Defendant to facilitate payment to them.

194. The monies for goods that Plaintiffs and Class Members paid to Defendant were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

195. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

196. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

197. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, requests judgment against the Defendant and that the Court grant the following:

A. An Order certifying the Nationwide Class, Indiana Subclass, New York Subclass, and California Subclass as defined herein, and appointing Plaintiffs and their counsel to represent the Classes;

B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and Class Members' PII;

C. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;

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

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's 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

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

Date: May 27, 2021

Respectfully Submitted,

By: */s/ Gary M. Klinger*

MASON LIETZ & KLINGER LLP
Gary M. Klinger
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (202) 429-2290
Facsimile: (202) 429-2294
gklinger@masonllp.com

FREEMAN & HERZ LLC
Carl V. Malmstrom
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 545-4653
malmstrom@whafh.com

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