UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

ANGELA GARRETT and CRYSTA GARNER on behalf of themselves and all others similarly situated,	
Plaintiffs,	
v.	**Case No. 1:21-cv-1329**
HERFF JONES, LLC,	**Putative Class Action**
Defendant.	

CLASS ACTION COMPLAINT

Plaintiffs Angela Garrett and Crysta Garner ("Plaintiffs") bring this Class Action Complaint, on behalf of themselves and all others similarly situated (the "Class"), against Defendant, Herff Jones, LLC ("Herff Jones" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge and experience:

NATURE OF THE CASE

1. Plaintiffs bring this class action against Herff Jones for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Herff Jones's customers' credit and debit card and other payment information from threat actors.

2. In 2021, the threat actors gained access to Herff Jones's payment card environment and payment systems (the "Data Breach"). The Data Breach included, at a minimum, information sufficient to make fraudulent transactions on Plaintiffs' and the Class Members' payment cards and accounts. Such information is believed to include, but not be limited to, first and last names, credit and debit card numbers, card expiration dates, security codes, billing addresses, shipping

addresses, ACH information, order numbers, and other financial information (collectively, "Payment Information").

3. The Data Breach has led to a flurry of fraudulent and unauthorized purchases on Herff Jones's customers credit and debit cards over the past few months. Herff Jones failed to safeguard Plaintiffs' and other customer's Payment Information and failed to inform them of the data breach until many of the customers reported a rash of fraudulent charges on their accounts after purchasing items from Herff Jones. Plaintiffs seek, among other things, damages, orders requiring Herff Jones to fully and accurately disclose the nature of the information that has been compromised, adopt reasonably sufficient security practices and safeguards to prevent incidents like the data breach at issue in the future, and provide identity theft protective services to Plaintiffs and Class Members for their lifetimes, as Plaintiffs and Class Members will be at an increased risk of identity theft due to the conduct of Herff Jones described herein.

4. Herff Jones markets and sells class rings, yearbooks, and commencement-related products, including but not limited to graduation caps, gowns, tassels, announcements, thank you notes, and diploma frames.

5. Herff Jones accepts payments from customers, like Plaintiffs, online and in person, including via debit and credit card for Herff Jones's products.

6. On May 13, 2021, several colleges and universities, including but not limited to, University of Houston, University of Illinois, Towson University, and University of Delaware began reporting that their students' and students' parents' bank accounts and/or Payment Information was being used to conduct fraudulent purchases.

7. Many additional colleges, universities, and schools have also reported that their students' and students' parents' Payment Information utilized for purchases from Herff Jones was

being used to make fraudulent purchases. Since the Data Breach, Herff Jones communicated that it was investigating the Data Breach and might have updates at a later point. As of May 12, 2021, Herff Jones has a red banner posted near the top of the homepage of its website titled, "HERFF JONES CYBER SECURITY INCIDENT UPDATE." Clicking on the hyperlinked banner returns a website stating, in part, "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." Herff Jones also states, "During the course of our investigation, which is ongoing, we identified theft of certain customers' payment information."

8. As a result of Herff Jones's failure to implement and follow basic security procedures, Plaintiffs' and Class Members' private Payment Information was and, in some cases continues to be, used by criminals to make fraudulent charges on Herff Jones's customers' payment cards. Plaintiffs and Class Members face a substantially increased risk of identity theft, both currently and for the indefinite future, at least in part because personal and Payment Information can now be offered for purchase to would be identity thieves in an aggregated format, lending itself, for example, for ease-of-use in widespread phishing email schemes. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Herff Jones's failures.

9. Plaintiffs, on behalf of themselves and all others similarly situated, allege claims for negligence, negligence *per se*, and declaratory judgment on behalf of the Nationwide Class (defined *infra*), the California Customer Records Act ("CCRA") on behalf of the California Subclass (defined *infra*), and the Illinois Consumer Fraud and Deceptive Practices Act ("Illinois CFA") on behalf of the Illinois Subclass (defined *infra*). Plaintiffs seek damages, reasonable

attorneys' fees, costs, and injunctive relief, including the adoption of reasonably sufficient practices to safeguard Payment Information remaining in Herff Jones's custody in order to prevent incidents like the Data Breach and further fraudulent transactions from reoccurring in the future.

PARTIES

10. Plaintiff Angela Garrett is a citizen and resident of the State of Illinois. Plaintiff Garrett made purchases from Heff Jones on April 15, 2021 relating to her May 23, 2021 graduation from Harold Washington College, located in Illinois. Plaintiff Garrett's purchases from Herff Jones were transacted in the State of Illinois on her Netspend debit card. Specifically, Plaintiff Garrett purchased the Grad Package 1 from Herff Jones including 10 Announcements, 25 Thank You Notes, Keepsake Announcement Cover, 30 Custom Return Address Labels, 25 Envelope Seals, 25 Tissues Inserts, HJ SmartShare10pk, Cap, Gown, Tassel, and Academic Diploma Frame for a total purchase amount of $229.20. On or about May 9, 2021, Plaintiff Garrett experienced 10 unauthorized transactions on her debit card named Changi Recommends Singapore in the amounts of $1.01, $104.21, $104.21, $104.21, $104.21, $52.61, $52.61, $52.61, $52.61, and $1.01, for a total of $627.28.

11. Plaintiff Garrett attempted to engage with Herff Jones to ascertain additional information about the Data Breach. Herff Jones's Customer Service associate, Autumn, stated on May 14, 2021, that the Data Breach "was being thoroughly investigated by our internal and third-party security experts," but that "the support team is not provided specifics on this issue and are unable to assist with any inquiries related to it."

12. Plaintiff Garrett had additional email communications with Herff Jones's agent, Freda Robinson, on May 20, 2021. Ms. Robinson advised Plaintiff Garrett that "[f]or the most current information concerning this matter, please visit our website at herffjones.com and click on

the red banner titled HERFF JONES CYBER SECURITY INCIDENT UPDATE. We sincerely apologize to those impacted by this incident."

13. As a result of the Data Breach, Plaintiff Garrett reviews her financial accounts more frequently than she did before the Data Breach. This review has been time-consuming, burdensome, and inconvenient. Furthermore, Plaintiff Garrett continues to worry about the Data Breach and was distressed as a result of having funds debited from her account. Plaintiff Garrett was looking forward to graduating from college along with the sense of accomplishment that comes with such a major life achievement, but was subjected to persistent worrying and distress because the funds in her account where substantially depleted due to the Data Breach.

14. Had Plaintiff Garrett known that Herff Jones had inadequate data security, she would not have used her debit card to make purchases from Herff Jones.

15. Plaintiff Crysta Garner is a citizen and resident of the State of California. Plaintiff Garner, while present in California, purchased graduation-related items from Herff Jones using her Mastercard credit card relating to her daughter's upcoming graduation from Mt. San Antonio College. On or about May 8, 2021, Plaintiff Garner discovered fraudulent purchase activity on her Mastercard credit card.

16. As a result of the Data Breach, Plaintiff Garner has spent and continues to spend considerable time and effort trying to protect her payment card account, including contacting her credit card provider to dispute the fraudulent charges and calling each place where fraudulent charges were made. This experience has caused Plaintiff Garner to worry and distress over the fraudulent charges that were attributed to her.

17. Had Plaintiff Garner known that Herff Jones had inadequate data security, she would not have used her credit card to make purchases from Herff Jones.

18. Since the announcement of the Data Breach, Plaintiffs have been required to spend their valuable time changing their Payment Information, including but not limited to, canceling payment cards, receiving new payment cards, contesting the fraudulent charges on their payment card accounts, and attempting to determine what other information was compromised in the Data Breach. Plaintiffs' time and efforts in undertaking these actions would not have occurred but for the Data Breach.

19. As a result of the Data Breach, Plaintiffs will continue to be at heightened risk for, spend time related to, and sustain damages from fraud and identity theft for years to come. Such risk (including risk of fraudulent transactions on their payment card accounts) is certainly impending and is not speculative, given that information from the Data Breach is already being used for fraudulent purposes by those who gained access to Herff Jones's systems containing Plaintiffs' and Herff Jones customers' sensitive Payment Information.

20. Defendant Herff Jones, LLC is a limited liability company organized in the State of Indiana with its principal place of business in Indianapolis, Indiana.

JURISDICTION AND VENUE

21. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiffs and at least one member of the Class, as defined below, are citizens of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

22. This Court has personal jurisdiction over Defendant because Defendant is organized and headquartered in the State of Indiana.

23. Pursuant to 28 U.S.C. § 1391(b)(1), venue is proper in this District because Defendant resides in this District.

FACTUAL BACKGROUND

Herff Jones

24. Herff Jones publicizes that it "started manufacturing class rings, medals, pins and other emblematic jewelry. As the years went by, the company has grown to include yearbooks, graduation announcements, diplomas, caps and gowns, and diploma frames."[1]

25. Herff Jones has "manufacturing facilities across the United States" and "is proud to be part of the part of commencement ceremonies and festivities for thousands of colleges and high school across the country and in Canada."[2] Herff Jones also provides products to "countless grade schools, middle schools, churches, sports team, movie studios and even courtrooms."[3]

26. At least hundreds of thousands of customers made purchases from Herff Jones this year in anticipation of school graduations.

Herff Jones Obtains, Collects, and Stores Plaintiffs' and Class Members' Information

27. In the ordinary course of doing business with its customers, Herff Jones collects customers' "(i) name; (ii) email address; (iii) age; (iv) postal address; (v) username and password associated with your account; (vi) phone numbers; (vii) measurements for uniform orders; and (viii) demographic information."[4] Additionally, Herff Jones notes that it "may also collect and maintain your billing address, shipping address, product selections, financial information (such as your credit or debit card information or ACH information, applicable card expiration dates and

[1] www.herffjones.com/about/ (last visited on May 21, 2021).
[2] *Id*.
[3] *Id*.
[4] https://www.herffjones.com/about/privacy/#info (last visited on May 21, 2021).

security codes) and your order number."[5] Plaintiffs and Class Members are regularly required to provide their sensitive, personal and private protected information in order to purchase Herff Jones's products.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Payment Information, Herff Jones assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Payment Information from disclosure. Indeed, Herff Jones notes that it has "implemented administrative, technical, and physical security measures to protect against the loss, misuse, and/or alteration of your information. These safeguards vary based on the sensitivity of the information that we collect and store."[6]

29. Relating to California customers, Herff Jones notes that under the California Consumer Privacy Act, it collects:

- identifiers (such as name, address, email address);
- commercial information (such as transaction data);
- financial data (such as credit card information collected by our payment processors on our behalf);
- internet or other network or device activity (such as browsing history or usage information);
- geolocation information (e.g., your approximate location based on IP address, or precise location with your consent for personalized advertising purposes);
- inference data about you (e.g., the additional services we think would be of most interest to you based on your interactions with us);
- legally protected classifications (such as gender and age);
- physical characteristics or description (e.g., measurements for uniform orders); and,
- other information that identifies or can be reasonably associated with you.[7]

[5] *Id*.
[6] https://www.herffjones.com/about/privacy/ (last visited on May 21, 2021).
[7] https://www.herffjones.com/about/privacy/#CA (last visited on May 21, 2021).

30. Plaintiffs and Class Members reasonably expect that service providers such as Defendant will use the utmost care to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

31. Despite Defendant's representation that it had implemented administrative, technical and physical security measures, Herff Jones failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' Payment Information.

32. Had Herff Jones remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Herff Jones could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Payment Information.

33. Plaintiffs and Class Members provided their Payment Information to Herff Jones with the reasonable expectation and mutual understanding that Herff Jones would comply with its obligations to keep the Payment Information confidential and would secure it from unauthorized access by intentional threat actors. However, Herff Jones failed to do so, in contravention of its own privacy policy.

34. Herff Jones further had a duty to protect Plaintiffs' and Class Members' confidential Payment Information under the Federal Trade Commission Act. The Federal Trade Commission ("FTC") has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act (codified by 15 U.S.C. § 45).

35. Furthermore, Herff Jones is prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

36. Beginning in 2007, the FTC released a set of industry standards related to data security and the data security practices of businesses, called "Protecting Personal Information: A Guide for Businesses" (the "FTC Guide").[8] In 2011, this guidance was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

- Businesses should dispose of personal identifiable information that is no longer needed;
- Businesses should encrypt personal identifiable information and protected cardholder data stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- Businesses should thoroughly understand the types of vulnerabilities on their network (of which malware on a point-of-sale system is one) and how to address said vulnerabilities;
- Businesses should implement protocols necessary to correct security breaches;
- Businesses should install intrusion detection systems to expose security breaches at the moment they occur;
- Businesses should install monitoring mechanisms to watch for massive troves of data being transmitted from their systems; and,
- Businesses should have an emergency plan prepared in response to a breach.

[8] *See FTC Unveils Practice Suggestions for Businesses on Safeguarding Personal Information*, FEDERAL TRADE COMM'N (Mar. 8, 2007), https://www.ftc.gov/news-events/press-releases/2007 /03/ftc-unveils-practical-suggestions-businesses-safeguarding; *see also* Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business, Federal Trade Commission* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal information.pdf (updated FTC Guide).

37. Herff Jones failed to adequately address the foregoing requirements in the FTC Guide.

38. In 2015, the FTC supplemented the FTC Guide once more with a publication called "Start with Security" (the "Supplemented FTC Guide").[9] This supplement added further requirements for businesses that maintain customer data on their networks:

- Businesses should not keep personal identifiable information and protected cardholder data stored on their networks for any period longer than what is needed for authorization;
- Businesses should use industry-tested methods for data security; and,
- Businesses should be continuously monitoring for suspicious activity on their network.

39. Again, Herff Jones failed to adequately address these requirements enumerated in the Supplemented FTC Guide.

40. The FTC Guide is clear that businesses should, among other things: (1) protect the personal customer information they acquire; (2) properly dispose of personal information that is no longer needed; (3) encrypt information stored on computer networks; (4) understand their network's vulnerabilities; and (5) implement policies for installing vendor-approved patches to correct security vulnerabilities. The FTC guidance also recommends that businesses: (1) use an intrusion detection system to expose a breach as soon as it occurs; (2) monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and (3) watch for large amounts of data being transmitted from the system.[10] Herff Jones did not follow these recommendations, and as a result exposed hundreds of thousands of consumers to harm.

[9] Fed. Trade Comm'n, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[10] *See, e.g.*, *id.*; Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

41. Furthermore, the FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

42. Herff Jones knew or should have known about its obligation to comply with the FTC Act, the FTC Guide, the Supplemented FTC Guide, and many other FTC pronouncements regarding data security.

43. Herff Jones's misconduct violated the FTC Act and the FTC's data security pronouncements, led to the Data Breach, and resulted directly and proximately in harm to Plaintiffs and Class Members.

Herff Jones Ignored the National Institute of Standards and Technology's Guidance

44. The National Institute of Standards and Technology provides basic network security guidance that enumerates steps to take to avoid cybersecurity vulnerabilities.[11] Although use of NIST guidance is voluntary, the guidelines provide valuable insights and best practices to protect network systems and data.

45. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.[12]

46. Herff Jones's failure to protect massive amounts of Payment Information throughout the multi-month breach period belies any assertion that Herff Jones employed proper data security protocols or adhered to the spirit of the NIST guidance.

---

[11] *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[12] *Id*. at Table 2 pg. 36-43.

Damages to Plaintiffs and Class Members Caused by the Data Breach

47. Plaintiffs and the Class Members have been damaged because their Payment Information was accessed by threat actors in the Data Breach. Plaintiffs and many Class Members have experienced fraudulent transactions on their payment cards and accounts after using the same Payment Information for legitimate purchases from Herff Jones.

48. Plaintiffs and certain Class Members have already incurred and will continue to incur out-of-pocket costs and expenses to potentially prevent them from suffering further harm. Plaintiffs and Class Members also have expended significant time and effort attempting to address the Payment Information that was disclosed to criminals in the Data Breach.

49. An expansive market exists online for stolen Payment Information, and Plaintiffs and Class Members have been damaged by having fraudulent transactions conducted on their payment cards and accounts and further stand at risk for fraudulent transactions.

50. Additionally, Plaintiffs and Class Members suffered "benefit of the bargain" damages because they overpaid for products that should have been sold by Herff Jones with the requisite and adequate data security. Unfortunately, such adequate data security was not afforded to Plaintiffs and the Class Members by Herff Jones.

51. Part of the price Plaintiffs and Class Members paid to Herff Jones was intended to be used to fund adequate data security. Thus, by way of the Data Breach, Class Members did not get what they paid for. Had Class Members known the truth about Herff Jones's deficient data security practices, they would not have used their payment cards at Herff Jones, or they would have been unwilling to pay full price for their purchases.

52. Plaintiffs and Class Members experiencing actual fraud are also harmed by the inability to use their credit or debit cards and other payment accounts when their accounts are

suspended or otherwise rendered unusable due to the fraudulent charges. Furthermore, Plaintiffs and Class Members are harmed via the loss of use of and access to their account and funds, or being limited in the amount of money they are permitted to obtain from their accounts, while fraudulent charges are investigated and not yet reversed. The time between when fraudulent charges are incurred and when they are reversed may take several days or weeks. Plaintiffs and Class Members are required to spend significant time and effort disputing fraudulent charges on their payment accounts as a result of the rash of fraudulent purchases caused by the Data Breach.

53. Plaintiffs and Class Members who experienced fraudulent card transactions may also be further harmed by being forced to relinquish rewards points or airline miles they earned on payment cards that were cancelled, or by not being able to earn points or miles on transactions they could not make on through their payment cards'while awaiting replacement cards.

54. Plaintiffs and Class Members who experienced fraudulent card transactions and lost access to stolen funds for days or weeks may also be harmed due to missed payments on bills and loans, late charges and fees, overdraft charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit marks caused by unpaid card bills.

55. Upon information and belief, the information obtained by the hackers through the Data Breach related to Plaintiffs and the Class Members is sufficient to provide those bad actors and other bad actors who have purchased or might purchase that information, the ability to open new credits cards and/or accounts in the Plaintiffs' and Class Members' names.

CLASS ALLEGATIONS

56. Plaintiffs bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following Class and Subclasses:

> **National Class:** All individuals in the United States whose Payment Information was compromised in the Herff Jones Data Breach which was disclosed in May 2021.
>
> **Illinois Subclass:** All residents of Illinois whose Payment Information was compromised in the Herff Jones Data Breach which was disclosed in May 2021.
>
> **California Subclass:** All residents of California whose Payment Information was compromised in the Herff Jones Data Breach which was disclosed in May 2021.

57. The National Class and Subclasses are collectively referred to herein as the "Class."

58. Excluded from the Class is Defendant, its subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representatives, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

59. Plaintiffs reserve the right to modify or amend the definition of the proposed Class if necessary before this Court determines whether certification is appropriate.

60. **Numerosity. Fed. R. Civ. P. 23(a)(1).** The requirements of Rule 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

61. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** The requirements of Rule 23(a)(2) and (b)(3) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting members of the Class. The

questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether Herff Jones's data security systems prior to and during the Data Breach complied with applicable data security laws, regulations, industry standards, and PCI DSS requirements;

b. Whether Herff Jones owed a duty to Class Members to safeguard their Payment Information;

c. Whether Herff Jones was negligent or reckless in permitting the Data Breach to occur;

d. Whether Herff Jones had and breached implied contractual obligations to Plaintiffs and Class Members;

e. Whether Herff Jones violated its own privacy policies and procedures;

f. Whether Herff Jones provided Plaintiffs and Class Members with adequate notification of the breach, and made available to them sufficient relief in response to it;

g. Whether Herff Jones breached its duty to Class Members to safeguard their Payment Information;

h. Whether a computer hacker obtained Class Members' Payment Information in the Data Breach;

i. Whether Herff Jones knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

62. **Typicality. Fed. R. Civ. P. 23(a)(3).** The requirements of Rule 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard Plaintiffs' and the Class Members' Payment Information.

63. Plaintiffs and Class Members were each Herff Jones's customers, each having their Payment Information obtained by an unauthorized third party.

64. **Adequacy. Fed. R. Civ. P. 23(a)(4).** The requirements of Rule 23(a)(4) are satisfied. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiffs and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class.

65. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class Member.

66. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** As the proposed Class includes at least hundreds of thousands of Herff Jones's customers, there is a significant risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Herff Jones. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing Herff Jones to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

67. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2). Class certification is also appropriate under Rule 23(b)(2).** Herff Jones, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive or declaratory relief appropriate for the Class as a whole. Moreover, upon information and belief, Herff Jones continues to maintain inadequate security practices, retains possession of Plaintiffs' and the Class Members' Payment Information, and has not been forced to change its practices or to relinquish Payment Information through other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue appropriate to the Class as a whole.

68. **Superiority. Fed R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when

damages to individual Plaintiffs and Class Members may not be sufficient to justify individual litigation. Here, damages suffered by Plaintiff and Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Herff Jones, and thus, individual litigation to redress Herff Jones's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

69. Particular issues are appropriate for certification under **Fed. R. Civ. P. 23(c)(4)** because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include those identified in Paragraph 61 above.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

70. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

71. Herff Jones owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Payment Information its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Herff Jones's security systems to ensure that Plaintiffs' and

Class Members' Payment Information in Herff Jones's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

72. Herff Jones's duty to use reasonable care arose from several sources, including but not limited to those described below.

73. Herff Jones had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable payment information that is routinely targeted by criminals for unauthorized access, Herff Jones was obligated to act with reasonable care to protect against these foreseeable threats.

74. Herff Jones admits that it has the responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the Payment Information at issue here.

75. Herff Jones breached the duties owed to Plaintiffs and Class Members and thus was negligent. Herff Jones breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Payment Information of Plaintiffs and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiffs' and Class Members' Payment Information in Herff Jones's possession had been or was reasonably believed to have been, stolen or compromised.

76. But for Herff Jones's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Payment Information would not have been compromised.

77. As a direct and proximate result of Herff Jones's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Payment Information;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Herff Jones Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Payment Information being placed in the hands of criminals;

h. Damages to and diminution in value of their Payment Information entrusted, directly or indirectly, to Herff Jones with the mutual understanding that Herff Jones would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their Payment Information, which remains in Herff Jones's possession and is subject to further breaches

so long as Herff Jones fails to undertake appropriate and adequate measures to protect Plaintiffs.

78. As a direct and proximate result of Herff Jones's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

79. Plaintiffs restate and reallege all proceeding factual allegations above and hereafter as if fully set forth herein.

80. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of companies like Herff Jones failing to use reasonable measures to protect Payment Information. Various FTC publications and orders also form the basis of Herff Jones's duty.

81. Herff Jones violated Section 5 of the FTC Act by failing to use reasonable measures to protect Payment Information and failing to comply with the industry standards. Herff Jones's conduct was particularly unreasonable given the nature and amount of Payment Information it obtained and stored and the foreseeable consequences of a data breach.

82. Herff Jones's violation of Section 5 of the FTC Act constitutes negligence *per se*.

83. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

84. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against

businesses which, as a result of their failure to employ reasonable data security measures, caused the same harm suffered by Plaintiffs and Class Members.

85. As a direct and proximate result of Herff Jones's negligence, Plaintiffs and Class Members have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

86. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

87. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

88. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' rights and obligations. Given that Plaintiffs and many Class Members have suffered fraudulent activity related to their person and financial information, the parties request guidance regarding whether Herff Jones is currently maintaining data security measures adequate to protect Plaintiffs' and Class Members from further data breaches that may compromise their Payment Information. Plaintiffs allege that Herff Jones's data security measures remain inadequate. Herff Jones publicly denies these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Payment Information and remain at imminent risk that further compromises of their Payment Information will occur in the future.

89. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Herff Jones owes a legal duty to secure consumers' Payment Information and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act; and

b. Herff Jones continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Payment Information.

90. This Court also should issue corresponding prospective injunctive relief requiring Herff Jones to employ adequate security protocols consistent with law and industry standards to protect consumers' Payment Information.

91. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Herff Jones. The risk of another such breach is real, immediate, and substantial. If another breach at Herff Jones occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified.

92. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Herff Jones if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Herff Jones of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Herff Jones has a pre-existing legal obligation to employ such measures.

93. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Herff

Jones, thus eliminating the additional injuries that would result to Plaintiffs and consumers whose Payment Information would be further compromised.

COUNT IV
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("Illinois CFA")
815 Ill. Comp. Stat. §§ 505/1, *et seq.*

94. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

95. This Count is brought on behalf of Plaintiff Angela Garrett and the Illinois Subclass.

96. Plaintiff Angela Garrett and the Illinois Subclass are "consumers" as that term is defined in 815 ILL. COMP. STAT. § 505/1(e).

97. Plaintiff Angela Garrett, the Illinois Subclass, and Defendant are "persons" as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

98. Defendant is engaged in "trade" or "commerce," including provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

99. Defendant engages in the "sale" of "merchandise" (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

100. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including but not limited to the following:

a. failing to maintain sufficient security to keep Plaintiff Garrett's and Subclass members' sensitive Payment Information from being hacked and stolen;

b. misrepresenting material facts to the Subclass, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Payment Information from unauthorized disclosure, release, data breaches, and theft;

c. misrepresenting material facts to the Subclass, in connection with sale of goods and services, by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' Payment Information; and

d. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Subclass members' Payment Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

101. In addition, Defendant's failure to disclose that its computer systems were not well-protected and that Plaintiff Garrett's and Illinois Subclass members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendant knew such facts would (a) be unknown to and not easily discoverable by Plaintiff Garrett and the Illinois Subclass; and (b) defeat Plaintiff Garrett's and Illinois Subclass members' ordinary, foreseeable and reasonable expectations concerning the security of their Payment Information on Defendant's servers.

102. Defendant intended that Plaintiff Garrett and the Illinois Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Defendant's offering of goods and services and incorporating

Plaintiff Garrett's and Illinois Subclass members' Payment Information on its servers, in violation of the Illinois CFA.

103. Defendant also engaged in unfair acts and practices by failing to maintain the privacy and security of Subclass members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

104. Defendant's wrongful practices occurred in the course of trade or commerce.

105. Defendant's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendant that applied to all Illinois Subclass members and were repeated continuously before and after Defendant obtained sensitive Payment Information and other information from Plaintiff Garrett and Illinois Subclass members. All Illinois Subclass members have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

106. Defendant also violated 815 ILL. COMP. STAT § 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILL. COMP. STAT § 530/1, et. seq., which provides, at Section 10:

> Notice of Breach.
>
> (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

107. 815 ILL. COMP. STAT § 530/20 provides that a violation of 815 ILL. COMP. STAT § 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

108. As a result of Defendant's wrongful conduct, Plaintiff Garrett and Illinois Subclass members were injured in that they never would have allowed their sensitive Payment Information – the value of which Plaintiff and Illinois Subclass members no long have control – to be provided to Defendant if they had been told or knew that Defendant failed to maintain sufficient security to keep such data from being hacked and taken by others.

109. Defendant's unfair and/or deceptive conduct proximately caused Plaintiffs Garrett's and Illinois Subclass members' injuries because, had Defendant maintained customer Payment Information with adequate security, Plaintiff Garrett and the Subclass members would not have lost it.

110. As a direct and proximate result of Defendant's conduct, Plaintiff Garrett and Subclass members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Defendant that Plaintiffs and class members would have never made had they known of Defendant's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Information, entitling them to damages in an amount to be proven at trial.

111. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiff Garrett seeks actual, compensatory, and punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the Illinois CFA.

COUNT V
CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")
Cal. Civ. Code §1798.80, *et seq.*

112. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

113. This Count is brought on behalf of Plaintiff Crysta Garner and the California Subclass.

114. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code §1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

115. Defendant is a business that maintains Personal Information about Plaintiff Garner and California Subclass members within the meaning of Cal. Civ. Code §1798.81.5. Such Personal Information includes, but is not limited to, the first and last names of Plaintiff Garner and the California Subclass, along with account numbers or credit or debit card numbers, in combination with any required security code, access code, or password that would permit access to Plaintiff Garner and the California Subclass's financial accounts. *See* Cal. Civ. Code §1798.81.5(d)(1)(A)(iii).

116. Businesses that maintain computerized data that includes Personal Information are required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code §1798.82(b). Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code §1798.82.

117. Defendant is a business that maintains computerized data that includes Personal Information as defined by Cal. Civ. Code §1798.80.

118. Plaintiff Garner's and California Subclass members' Personal Information includes Personal Information as covered by Cal. Civ. Code §1798.82.

119. Because Defendant reasonably believed that Plaintiff Garner's and California Subclass members' Personal Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach, immediately following its discovery, to the owners or licensees of the Personal Information (*i.e.*, Plaintiff Garner and the California Subclass) as mandated by Cal. Civ. Code §1798.82.

120. By failing to disclose the Data Breach immediately following its discovery, Defendant violated Cal. Civ. Code §1798.82.

121. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §1798.81.5 and 1798.82, Plaintiff Garner and California Subclass members suffered damages, as described above and as will be proven at trial.

122. Plaintiff Garner and California Subclass members seek relief under Cal. Civ. Code §1798.84, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and all other similarly situated, pray for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Respectfully Submitted,

/s/ Kathleen A. DeLaney
DELANEY & DELANEY, LLC
Kathleen A. DeLaney
3646 Washington Blvd.
Indianapolis, IN 46205
Phone: (317) 920-0400
Fax: (317) 920-0404
kathleen@delaneylaw.net

GOLDENBERG SCHNEIDER, LPA
Jeffrey S. Goldenberg (*Pro Hac Vice Forthcoming*)
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Phone: (513) 345-8291
Fax: (513) 345-8294
jgoldenberg@gs-legal.com

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner (*Pro Hac Vice Forthcoming*)
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

MARKOVITS, STOCK & DEMARCO, LLC
Terence R. Coates (*Pro Hac Vice Forthcoming*)
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Attorneys for Plaintiffs