

ASSURANCE OF DISCONTUANCE

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12), and General Business Law (“GBL”) §§ 349, 899-aa and 899-bb, into a data security incident at Herff Jones, LLC (“Herff Jones” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of the investigation and the relief agreed to by Herff Jones.¹

FINDINGS

1. Herff is a limited liability company, based in Indianapolis, Indiana that engages in trade or commerce by producing and selling yearbooks, class rings, caps and gowns, graduation announcements, maps, and awards.
2. In connection with the sale of its goods and services, Herff stored, processed, transmitted and received payment card information from its customers prior to April 2021.
3. On December 15, 2020, an unauthorized actor exploited a vulnerability in Lucee, a scripting language, to gain access to Herff’s web servers.
4. On April 7, 2021, Herff received a common point of purchase alert from one of its payment processors. The processor found “a number of cards tracing back to Herff on three different web sites, which are known to sell stolen card data.” After notification, Herff disabled access to systems exploited by the attacker, activated its incident response plan, and engaged a forensic investigator.
5. On April 12, 2021, Herff’s vulnerability detection software and management vendor identified and assisted in patching the Lucee vulnerability.

¹ The Commonwealth of Pennsylvania, by the Office of Attorney General by Attorney General Josh Shapiro, opened an investigation with NYAG, and entered into an Assurance of Voluntary Compliance with Herff with the same terms (collectively, “Attorneys General”).

6. Herff's investigation revealed the unauthorized actor exfiltrated the data of at least 206,925 cardholders, including names, credit card numbers, CVVs, expiry dates, email addresses, addresses, and phone numbers. Furthermore, an intelligence provider retained by Herff found approximately 383,610 payment cards for sale on the dark web that are potentially attributable to this incident.

7. During the exfiltration window, 30,295 Pennsylvania residents and 49,228 New York residents made transactions with Herff. The company began notifying affected consumers on June 15, 2021 and offered complimentary credit monitoring and identity protection services.

8. In investigating the Breach, a third-party Payment Card Industry Forensic Investigator found three violations of Payment Card Industry Data Security Standards.

9. Herff represented to its customers that it maintained administrative, technical, and physical security measures to protect against the loss, misuse and/or alteration of their information.

10. The Attorneys General allege that Herff failed to employ reasonable data security measures.

11. The Attorneys General allege Herff's conduct constitutes violations of the Consumer Protection Acts and Personal Information Protection Act (both as defined below).

PROSPECTIVE RELIEF

12. For the purposes of this Assurance, the following definitions will apply:

a. **“Cardholder Data Environment”** (“CDE”) has the same meaning as “cardholder data environment” as stated in the then current version of the PCI DSS.

b. **“Compensating Controls”** means alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the Chief Information Security Officer (“CISO”) or his or her designee to be impractical to

implement at the present time due to legitimate technical or business constraints. Such alternative mechanisms must: (1) meet the intent and rigor of the original stated requirement; (2) provide a similar level of security as the original stated requirement; (3) be up-to-date with current industry accepted security protocols; and (4) be commensurate with the additional risk imposed by not adhering to the original stated requirement. The determination to implement such alternative mechanisms must be accompanied by written documentation demonstrating that a risk analysis was performed indicating the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable, and that the CISO or his or her designee agrees with both the risk analysis and the determination that the risk is acceptable.

c. **“Consumer”** means any Pennsylvania or New York resident who purchases goods directly from Herff.

d. **“Consumer Protection Acts”** mean Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, *et seq.* and New York General Business Law § 349 and Executive Law § 63(12).

e. **“Effective Date”** will be December 14, 2022.

f. **“Payment Card Information”** (“PCI”) means Cardholder Data and Sensitive Authentication Data as defined by the PCI DSS.

g. **“Payment Card Industry Data Security Standard”** (“PCI DSS”) means the active and applicable version of the Payment Card Industry Data Security Standard published by Payment Card Industry Security Standards Council.

h. **“Personal Information Protection Act”** means New York General Business Law § 899-bb.

i. **“Sensitive Personal Information”** means information contained within the CDE of Consumers that is PCI and “personal information” of Consumers as defined under

the Breach of Personal Information Notification Act, 73 P.S. § 2302 (enacted December 22, 2005).

APPLICATION

13. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance apply to Herff, its affiliates, subsidiaries, successors and assigns, and its officers and employees in the scope of the performance of their job duties for Herff.

14. Herff must comply with the Consumer Protection Acts and Personal Information Protection Act in connection with its collection, use, and maintenance of Sensitive Personal Information, and shall maintain reasonable security policies and procedures designed to safeguard Sensitive Personal Information from unauthorized use or disclosure.

15. Herff must not misrepresent the extent to which it maintains and protects the privacy, security, confidentiality, or integrity of Sensitive Personal Information collected from or about Consumers.

16. Herff must develop, implement, and maintain a comprehensive information security program to govern the CDE (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Sensitive Personal Information Herff collects, stores, transmits, and/or maintains, and that must, at a minimum include the requirements set forth in this Assurance to the extent appropriate based on Herff’s assessment of relevant risks.

17. The Information Security Program includes the following components:

a. Documented methods and criteria for managing information security risks to Sensitive Personal Information, including assessment, prioritization, reduction, and acceptance of risks. The risk assessment methods and risk assessment criteria must conform to an information security risk assessment method that is provided by information security bodies (e.g., NIST Special Publications 800-30, The Sedona Conference Commentary on a Reasonable Security Test

(February 2021), ISO 27005, Duty of Care Risk Analysis Standard (“DoCRA”), or Center for Internet Security Risk Assessment Method (“CIS RAM”) Version 2.0), and achieving the control objectives listed below:

- i. The safeguards must not create a likelihood and impact of harm to Consumers or the public interest such that a remedy is needed.
- ii. The safeguards may not require Herff to curtail its proper objectives (e.g., profit, growth, reputation, market competitiveness) or the utility of Herff’s services to Consumers.
- iii. The burden imposed on Herff by the safeguards must be proportionate to the risk the safeguards reduce to Consumers and the public interest.

b. Herff must conduct such security risk assessments inclusive of the CDE and any network where Herff stores Sensitive Personal Information at least annually. Within a reasonable period of time after changes to the security of its CDE or any other network where Herff stores Sensitive Personal Information that may significantly increase risks to Consumers, Herff will assess the impact of the change. Comprehensive assessments will include foreseeable threats to Sensitive Personal Information. Risk assessments will be conducted by parties that are competent to model threats that are relevant to Herff and who may capably help to address risks that are created by those threats.

c. Information Security Program Assessment: At least annually, Herff must continue to review the effectiveness of Herff’s Information Security Program.

18. Such Information Security Program must be developed and implemented within one hundred eighty (180) days after the Effective Date of this Assurance. For any requirements not fully developed and implemented within one hundred eighty (180) days after the Effective Date of this Assurance, Herff must implement interim Compensating Controls to address the identified risks.

19. Herff's Information Security Program must be written and contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Herff's operations; (ii) the nature and scope of Herff's activities; and (iii) the sensitivity of the Sensitive Personal Information that Herff maintains.

20. Herff must designate a qualified individual (e.g., employee, independent contractor, shared services resource) with appropriate credentials, background, and expertise in information security who will be responsible for overseeing Herff's implementation and maintenance of the Information Security Program. The duties and responsibilities of the qualified individual must be documented and include advising senior leadership, which may include the Chief Executive Officer and the Board of Directors of Herff's security posture, security risks and security remediation and resiliency strategy.

21. Herff's Information Security Program must include security awareness training to all personnel with key responsibilities for implementation and oversight of the Information Security Program. Herff's training must ensure that system, database, and network administrators, and persons with privileged access to the CDE are fully informed of the requirements of the Information Security Program relevant to their functions, which may include password policies, secure data handling, secure storage, transmission and disposal of Sensitive Personal Information, and reasonable practices designed to prevent attackers from obtaining credentials and other sensitive data through malicious downloads and other threats identified in the annual or other comprehensive risk assessment. Within ninety (90) days of the Effective Date, Herff will provide training required by this Assurance, and thereafter will provide the training to covered personnel on at least an annual basis.

INFORMATION SECURITY SAFEGUARDS

22. As part of the Information Security Program, Herff must implement reasonable security for Sensitive Personal Information, including:

a. Herff must reasonably know the actual and intended location and disposition of Sensitive Personal Information. Herff may achieve this objective through the use of process diagrams and procedures, information classification procedures, data scanning and inventory systems, asset scanning or management systems, or other means.

b. Herff must take reasonable steps to ensure that it installs and uses only approved software that it maintains and keeps updated.

c. Herff will maintain a software patch management program that includes the use of automated, standardized patch management distribution tool(s), whenever technically feasible, to deploy patches to endpoints, verify patch installation, and retain patch history.

d. Herff must develop, implement, and maintain a penetration-testing program designed to identify, assess, and remediate identified security vulnerabilities. Herff will achieve this objective by conducting and implementing regular penetration testing and reasonable remediation practices.

e. Herff must technologically segment the CDE from other areas of Herff's information technology operations.

f. Herff must employ reasonable measures to detect, investigate, contain, respond to, eradicate, and recover from security incidents within reasonable time periods. Such reasonable measures may include but are not limited to some or all of the following: log correlation and alerting, file integrity monitoring, data integrity monitoring, SIEM systems, intrusion detection, prevention systems, threat management systems, a

documented incident response plan, trained personnel, experts, or tools that sufficiently address the risks of harm cause by security incidents.

g. Herff must implement reasonable access controls in relation to systems in the CDE. Such reasonable access controls may include but are not limited to some or all of the following: multi-factor authentication, one-time passcodes, location-specific requirements, or other control enhancements.

23. Herff must comply with PCI DSS with respect to its CDE.

24. Herff must validate PCI DSS compliance for its CDE by engaging a PCI Qualified Security Assessor to conduct an assessment resulting in the delivery of a PCI Report on Compliance and Attestation of Compliance.

SETTLEMENT COMPLIANCE ASSESSMENT

25. Within one (1) year of the Effective Date and biennially for five (5) years from the first compliance assessment, Herff must obtain assessments of its Information Security Program. The assessments must be performed by a qualified and independent third party that has at least five (5) years of experience evaluating the effectiveness of computer systems or information system security. The assessments must set forth the administrative, technical, and physical safeguards maintained by Herff and explain whether the safeguards are reasonable in relation to Herff's size and complexity, the nature and scope of Herff's activities, and any Sensitive Personal Information that Herff collects, stores, transmits, and/or maintains.

PAYMENT

26. Herff will pay two hundred thousand dollars (\$200,000.00) to the Attorneys General. Said payment will be divided and paid by Herff directly to each of the Attorneys General in an amount designated by the Attorneys General and communicated to Herff by the Attorneys

General. Payment must be made no later than thirty (30) days after the Effective Date of this Assurance and receipt of such payment instructions by Herff from the Attorneys General.

27. The payments received by the Attorneys General may be used for purposes that may include, but are not limited to, attorneys' fees, and other costs of investigation and litigation, or may be placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education or redress, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, and/or for other uses permitted by state law.

28. Nothing in this Assurance will be construed to limit the authority or ability of the Attorneys General to protect the interests of his/her State or the people of his/her State. This Assurance will not bar the Attorneys General or any other governmental entity from enforcing laws, regulations, or rules against Herff for conduct subsequent to or otherwise not covered by the Release. Further, nothing in this Assurance will be construed to limit the ability of the Attorneys General to enforce the obligations that Herff has under this Assurance.

MISCELLANEOUS

29. Respondent expressly agrees and acknowledges that NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 35, and agrees and acknowledges that in the event the Assurance is voided:

- a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;
- b. the NYAG may use statements, documents or other materials produced or provided by Respondent prior to or after the Effective Date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

30. If a court of competent jurisdiction determines that Respondent has violated the Assurance, Respondent shall pay to the NYAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

31. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondent. Respondent shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of NYAG.

32. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

33. Any failure by the NYAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Respondent.

34. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 22-081, and shall be in writing and shall, unless expressly provided

otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent, to:

Ken Moore
SVP and Chief Technology Officer
Herff Jones, LLC
4625 W 62nd Street
Indianapolis, IN 46268

Copy to:

Antony Kim
Jennifer Archie
Latham & Watkins LLP
555 Eleventh Street, NW, Suite 1000
Washington, D.C. 20004

If to NYAG, to:

Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005
ifraud@ag.ny.gov

35. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondent and its counsel and NYAG's own factual investigation as set forth in NYAG's Findings, paragraphs 1-10 above. Respondent represents and warrants that neither it nor its counsel has made any material misrepresentations to NYAG. If any material misrepresentations by Respondent or its counsel are later found to have been made by NYAG, this Assurance is voidable by NYAG in its sole discretion.

36. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondent in agreeing to this Assurance. This Assurance is not intended for use by any third party in any other proceeding.

37. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

38. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

39. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that Respondent violates the Assurance after its Effective Date.

40. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

41. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

42. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

43. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

44. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

45. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as


of the Effective Date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

<p>LETITIA JAMES ATTORNEY GENERAL OF THE STATE OF NEW YORK</p> <p>By: /s Clark Russell _____</p> <p>Clark Russell Deputy Bureau Chief Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005</p> <p>12.15.22 _____</p> <p>Date</p>	<p>HERFF JONES, LLC</p> <p>By: _____</p> <p>Ken Moore SVP and Chief Technology Officer Herff Jones, LLC 4625 W 62nd Street Indianapolis, IN 46268</p> <p>_____</p> <p>Date</p>
--	---

of the Effective Date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

<p>LETITIA JAMES ATTORNEY GENERAL OF THE STATE OF NEW YORK</p> <p>By: _____</p> <p>Clark Russell Deputy Bureau Chief Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005</p> <p>_____ Date</p>	<p>HERFF JONES, LLC</p> <p>By: </p> <p>Ken Moore SVP and Chief Technology Officer Herff Jones, LLC 4625 W 62nd Street Indianapolis, IN 46268</p> <p><u>December 5, 2022</u> Date</p>
---	---