ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 23-022

Investigation by LETITIA JAMES,
Attorney General of the State of New York, of

Sports Warehouse Properties Georgia LLC;
Sports Warehouse, Inc., d/b/a Tennis Warehouse, LLC; Wilderness Sports Warehouse, LLC, d/b/a Tackle Warehouse; Skate Warehouse, LLC; and Running Warehouse, LLC,

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (the "OAG") commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12) and General Business Law ("GBL") §§ 899-aa and 899-bb into a data security incident at Sports Warehouse Properties Georgia LLC; Sports Warehouse, Inc., d/b/a Tennis Warehouse, LLC; Wilderness Sports Warehouse, LLC, d/b/a Tackle Warehouse; Skate Warehouse, LLC; and Running Warehouse, LLC (collectively, the "Sports Warehouse Entities" or "Respondents") (together with the OAG, the "Parties"). This Assurance of Discontinuance ("Assurance") contains the findings of the OAG's investigation and the relief agreed to by the OAG and the Sports Warehouse Entities.

FINDINGS OF OAG

1. Respondents, the Sports Warehouse Entities, are related entities based in San Luis Obispo, CA that have operated a series of online storefronts selling sporting goods to consumers, including tennis-warehouse.com, runningwarehouse.com, skatewarehouse.com, and tacklewarehouse.com (together, the "Sports Warehouse Websites"), since at least 2002.

Although the Sports Warehouse Entities are legally separate entities, they share all IT infrastructure, policies and procedures, and personnel.

2. Like most retail websites, the Sports Warehouse Websites allow customers to create online accounts by entering an email address and choosing a password.

3. Between approximately 2002 and 2021, the Sports Warehouse Entities processed consumers' online credit card transactions through a credit card processor via the Sports Warehouse Websites. As a result, the Sports Warehouse Entities had access to consumers' payment card information, much of which they stored indefinitely on their servers.

The 2021 Data Breach

4. On October 15, 2021, Respondents received an unsolicited contact from Gemini Advisory, a fraud intelligence advisory firm who was not contracted by Respondents, who advised that customer payment card data that appeared to have been used on the Sports Warehouse Websites had been posted for sale on the dark web. This customer information included Card Verification Values ("CVVs"), card holder names, and billing address information. Subsequently, the Sports Warehouse Entities were contacted by U.S. Homeland Security Investigations ("HSI"), which had found payment card information that had a common point of purchase from the Sports Warehouse Websites for sale on the dark web. Around the same time, Respondents also received an inquiry from the U.S. Secret Service ("USSS") regarding the Sports Warehouse Websites. Respondents engaged with HSI and USSS and obtained information about their investigations into the matter.

5. On October 27, 2021, Fiserv, the Sports Warehouse Entities' payment processor, informed them that Mastercard had requested that Respondents engage a Payment Card Industry ("PCI") approved Forensic Investigator ("PFI") to conduct a PCI investigation due to the

issuance to Fiserv of two fraud alerts known as a common point of purchase ("CPP") reports from a large credit card company that had linked fraud on multiple of its customers' accounts back to earlier purchases the customers had made on the Sports Warehouse Websites.

6. On November 1, 2021, Respondents engaged a PFI to conduct the required PCI investigation. The PFI confirmed that attackers had gained access to certain of Respondents' systems on or about October 1, 2021, and had obtained customers' payment card information, including consumer names, addresses, card number, CVVs, and expiration dates.

7. In the report of its investigation, the PFI concluded that:

a. The attackers appeared to have conducted a brute force attack on Respondents' servers between September 10 and 11, 2021, that had gained them access to the admin page of Respondents' "Lists" web server, which was protected by only single factor authentication (*i.e.*, a password);

b. The attackers subsequently created web shells on the Sports Warehouse Entities' servers, including utilizing a known Web Shell by Orb from a publicly available Github repository;

c. The attackers were able to transit their web shells from the Sports Warehouse Entities' file server, which they originally accessed, to the ecommerce server where they used their web shells to access, compress, download, and then delete files that contained the order information used for backend processing by Respondents, including most credit card data, for every purchase made through the Sports Warehouse Websites since at least 2002;

d. The Sports Warehouse Entities had stored the subsequently exfiltrated payment card data on their servers in plain text; and,

e. The PFI concluded that the attacker had been able to move laterally between the Sports Warehouse Entities' Lists server and their e-commerce server(s) containing payment card information due to the existence of shared passwords and a lack of complete segmentation.

8. After the PFI report had been completed, the Sports Warehouse Entities continued to investigate the attack. The Sports Warehouse Entities later concluded that attackers had also accessed certain customers' login credentials (*i.e.*, email address and password) for the Sports Warehouse Websites on the same e-commerce server.

9. Respondents ultimately concluded that the attackers had potentially accessed the non-expired payment card information of as many as 1,813,224 consumers, including 101,558 New Yorkers, and the login credentials of 1,180,939 consumers, including 82,757 New Yorkers.

10. Beginning on December 16, 2021, Respondents notified affected customers whose credit card information had been affected by the attack.

11. Beginning on April 11, 2021, Respondents notified affected customers whose login credentials had been affected by the attack and who resided in relevant jurisdictions.

12. Respondent neither admits nor denies OAG's Findings, paragraphs 1-11 above.

13. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL §§ 899-aa & 899-bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

RELIEF

14. For the purposes of this Assurance, the following definitions shall apply:

a. "Customer" shall mean any individual who resides in New York who initiates a purchase of or purchases goods or services from the Sports Warehouse Entities or any individual who resides in New York who otherwise provides Private Information to the Sports Warehouse Entities in connection with an authorized transaction on the Sports Warehouse Websites.

b. "Private Information" shall have the same meaning as the same term in New York General Business Law § 899-aa.

GENERAL COMPLIANCE

15. Respondents shall comply with Executive Law § 63(12), and GBL §§ 899-aa & 899-bb, in connection with their collection, use, and maintenance of Private Information.

INFORMATION SECURITY PROGRAM

16. Respondents shall maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Customer Private Information that Respondents collect, store, transmit, and/or maintain. Respondents shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include the following processes:

a. Assess and document, not less than annually, internal and external risks to the security, integrity and confidentiality of Customer Private Information;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondents identified that are appropriate to: (i) the size and complexity of Respondents' operations; (ii) the nature and scope of Respondents' activities; and (iii) the

volume and sensitivity of the Customer Private Information that Respondents collect, store, transmit, and/or maintain;

c. Assess, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks Respondents identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with (b) above; and,

d. In circumstances where service providers will be provided access to or entrusted with Customer Private Information, select service providers capable of reasonably safeguarding Customer Private Information, contractually require service providers to implement and maintain appropriate safeguards to protect Customer Private Information, and take appropriate steps to verify service providers are complying with the contractual requirements.

17. Respondents shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program (the "Chief Information Security Officer[1]"). The Chief Information Security Officer shall report at a minimum quarterly to the Chief Executive Officer (or the equivalent thereof) and senior management concerning Respondents' security posture, the security risks faced by Respondents, and the Information Security Program. The Chief Information Security Officer shall report at a minimum semi-annually to the Board of Directors (or the equivalent thereof) regarding the same.

[1] Respondents need not use this title for the individual. The title used here is for identification purposes only.

18. Respondents shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within one hundred twenty (120) days of the Effective Date of this Assurance, or within sixty (60) days of when an employee first assumes new responsibility for implementing, maintaining, or monitoring the Information Security Program.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

19. Encryption: Respondents shall encrypt or cause their relevant vendors to encrypt Private Information that they collect, use, store, transmit and/or maintain, whether stored within Respondents' Network, or transmitted electronically within or outside the Respondents' Network, using a reasonable encryption algorithm where technically feasible.

20. Customer Password Management: Respondents shall, to the extent they have not already done so, establish, and, thereafter, maintain appropriate password policies and procedures for Customer accounts. Such policies and procedures shall include strong password requirements (at least 8 characters, with at least one capital letter, one lowercase letter and one symbol or number) and shall include hashing stored passwords using a hashing algorithm and salting policy at a minimum commensurate with reasonable standards and security risks that are known or reasonably should be known, given the size and nature of the business.

21. Anti-Malware Program: Respondents shall implement, maintain, and regularly monitor, test, and update reasonable anti-malware protections such as an EDR solution or reasonably equivalent technology generally utilized in similar circumstances in an Apple based environment.

22. Logging & Monitoring: Respondents shall, to the extent they have not already done so, establish, and, thereafter, maintain, or cause their relevant vendors to maintain, a system designed to collect and monitor network activity significant and relevant to the security of Respondents' systems, such as through the use of security and event management tools, as well as policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (1) provide for centralized logging and monitoring of activity significant and relevant to the security of Respondents' systems on Respondents' network, and (2) monitor for and alert security personnel to suspicious activity. Logs for network activity should be actively accessible and stored for defined periods set by Respondents' record retention policy and that are sufficient to provide support for after-the-fact investigations of incidents.

23. Penetration Testing: Respondents shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities within Respondents' computer network. This program shall include regular penetration testing, risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards for the size and nature of the business.

24. Network Vulnerability Scanning: Respondents shall regularly run comprehensive internal and external vulnerability scans of its network not less than quarterly. Scans shall be performed by qualified employees or vendors.

25. Data Collection: Respondents shall request, collect, use, or store Private Information only to the extent reasonably necessary to accomplish the intended legitimate business purpose for collection.

26. Data Deletion: Respondents shall use reasonable efforts to permanently and securely delete or otherwise dispose of Private Information when, in the reasonable determination of Respondents, there is no current or foreseeable business or legal purpose to retain it.

INFORMATION SECURITY PROGRAM ASSESSMENTS

27. For a period of three (3) years from the Effective Date, Respondents shall provide to the OAG copies of the following within two weeks of completion:

a. An annual third-party assessment of Respondents' systems, networks, and/or policies concerning information security, which may consist of a third-party PCI compliance assessment and any penetration testing pursuant to paragraph 23; and,

b. Any other assessments pertaining to Respondents' PCI compliance that may be conducted, which may be redacted to avoid the exposure of sensitive security information that could create a security risk.

MONETARY RELIEF

28. Respondents shall pay to the State of New York three hundred thousand dollars ($300,000.00) in penalties (the "Monetary Relief Amount"). Payment of the Monetary Relief Amount shall be made in full within fourteen (14) days of the Effective Date of this Assurance. Any payment shall reference AOD No. 23-022.

MISCELLANEOUS

29. Respondents expressly agree and acknowledge that the OAG 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 36, and agrees and acknowledges that in such event:

a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;

b. the OAG may use statements, documents or other materials produced or provided by the Respondents 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 Respondents 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 the Respondents have violated the Assurance, the Respondents shall pay to the OAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

31. This Assurance is not intended for use by any third party in any other proceeding.

32. Acceptance of this Assurance by the OAG is not an approval or endorsement by the OAG of any of Respondents' policies, practices, or procedures, and the Respondents shall make no representation to the contrary.

33. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondents. Respondents shall include 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 the OAG.

34. Any failure by the OAG to insist upon the strict performance by Respondents of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, 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 the Respondents.

35. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-022, 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 the Respondents, to:

Drew Munster, or in his/her absence, to the person holding the title of
CEO
Sports Warehouse
181 Suburban Road

San Luis Obispo, CA 93401
drew@tennis-warehouse.com

If to the OAG, to:

Laura Mumm, Assistant Attorney General, or in her absence, to the person holding the title of Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005
Laura.Mumm@ag.ny.gov

36. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondents and their counsel and the OAG's own factual investigation as set forth in Findings, paragraphs (1)-(11) above. The Respondents represent and warrant that neither they nor their counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by Respondents or their counsel are later found to be inaccurate or materially misleading, this Assurance is voidable by the OAG in its sole discretion.

37. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondents in agreeing to this Assurance.

38. The Respondents represent and warrant, through the signatures below, that the terms and conditions of this Assurance are duly approved. Respondents further represent and warrant that Sports Warehouse, Inc., by Drew Munster], as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of the Sports Warehouse Entities.

39. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondents' obligations under this Assurance are enduring. Nothing in this Agreement

shall relieve Respondents of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

40. Respondents agree not to take any action or to make or authorize to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis.

41. Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that the Respondents violate the Assurance after its Effective Date.

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

43. 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 the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

44. Respondents acknowledge that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

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

46. 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.

47. 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. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

48. The Effective Date of this Assurance shall be the date of the last signature to this agreement.

LETITIA JAMES
Attorney General of the State of New York
28 Liberty Street
New York, NY 10005

By: _____
Laura C. Mumm
Assistant Attorney General
Bureau of Internet & Technology
Office of the New York State Attorney General
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433

Date: May 24, 2023

Sports Warehouse Properties Georgia LLC; Sports Warehouse, Inc., d/b/a Tennis Warehouse, LLC; Wilderness Sports Warehouse, LLC, d/b/a Tackle Warehouse; Skate Warehouse, LLC; and Running Warehouse, LLC

By: DocuSigned by: Drew Munster BE12A6E57B32464...
Drew Munster

Title: CEO, Sports Warehouse, Inc

Date: May 12, 2023