STATE OF COLORADO
DEPARTMENT OF LAW

ASSURANCE OF DISCONTINUANCE

IN THE MATTER OF SAVORY SPICE SHOP, LLC

This Assurance of Discontinuance ("Assurance") is entered into between the State of Colorado, *ex rel.* Philip J. Weiser, Attorney General for the State of Colorado ("the State"), and Savory Spice Shop, LLC ("Savory") pursuant to the Attorney General's powers under Colo. Rev. Stat. section 6-1-110(2) and constitutes a complete settlement between the State and Savory (the "Parties") regarding the State's allegations as to the security breaches that Savory detected on September 17, 2020 and March 27, 2021.

I. INTRODUCTION

Cybercrime and identity theft harm Colorado residents. Unsecure e-commerce websites can lead to many types of cybercrimes, one of which is payment card skimming. Online payment card skimming happens when a criminal infects a website's checkout page with malware to steal payment card information. Criminals can then use this information to make fraudulent charges. Payment card fraud impacts consumers' savings, livelihoods, and credit scores. Consumers must sometimes engage in stressful and time-consuming processes to secure their online identity and recoup fraudulently spent funds.

As online shopping continues to grow, it is critical that businesses secure their e-commerce websites. Colorado law requires companies that maintain sensitive personal information to take reasonable steps to protect the information and to notify Colorado residents promptly when their information is at risk of being misused.

Savory is based in Denver, Colorado and manages an e-commerce website and retail locations throughout the United States. Savory maintained payment card information of Colorado residents when it collected this information on its website's checkout page to complete customer transactions. Savory failed to implement proper technical and administrative safeguards, leaving its website vulnerable to attack.

Savory was the victim of a cyberattack in which a criminal monitored and copied customer payment card information entered into Savory's checkout webpage. Savory's inadequate data security practices allowed the criminal to steal the payment card information of Savory's customers, including Colorado residents, for an unknown period of time before Savory's third-party payment card processor alerted Savory.

Due to Savory's delayed notice, affected Coloradans may have experienced payment card fraud or were unaware that their information had been compromised until they received notice ten months after Savory discovered the breach. The Parties enter into this Assurance to ensure Savory's future compliance with Colorado's data security laws.

II. PARTIES

1. Philip J. Weiser is the duly elected Attorney General for the State of Colorado and has express jurisdiction to investigate and prosecute violations of the Colorado Consumer Protection Act ("CCPA"), C.R.S. sections 6-1-101 through 6-1-1121.

2. Savory is a Colorado-based business with a principal office address of 1805 E. 58th Ave. Unit C, Denver, Colorado 80216.

III. DEFINITIONS

3. The term "Appropriate Standard" means a cybersecurity standard or controls set by the Payment Card Industry, National Institute of Standards and Technology (NIST), SANS Institute, International Organization for Standardization (ISO), or a data security standard of comparable scope and thoroughness.

4. The terms "Personal Identifying Information" and its abbreviation, "PII," include all of the items set forth in C.R.S. sections 6-1-713(1)(b) and 6-1-716(1)(g).

5. The term "Effective Date" means the first date upon which both Parties have executed and delivered this Assurance.

6. Unless otherwise specified, all definitions found in C.R.S. sections 6-1-105(1), 6-1-713(2), and 6-1-716(1) are incorporated herein, and any term defined in those sections shall have the same meaning when used in this Assurance.

IV. STATE'S ALLEGATIONS

A. Colorado's Data Security Laws.

7. C.R.S. section 6-1-713 requires companies that maintain, own, or license paper or electronic documents containing personal identifying information ("PII") to develop a written policy for the destruction or proper disposal of those paper and electronic documents when they are no longer needed.

8. C.R.S. section 6-1-713.5 requires companies that maintain, own, or license PII of Colorado residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII and the nature and size of the business and its operations.

9. C.R.S. section 6-1-716 imposes obligations on companies that experience security breaches or potential security breaches. When a company becomes aware that a security breach may have occurred, the company must "conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused." *Id.* § 716(2). The company "shall give notice to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur." *Id.* The company must give notice to residents in "the most expedient time possible, but no later than thirty days after the date of determination that a security breach occurred." *Id.*

B. Factual Allegations.

10. Savory maintained, owned, or licensed PII, including payment card information of Colorado residents because Savory collected customer payment card information on its checkout webpage and transferred the information to its third-party payment processor to complete online transactions.

11. Because Savory is a merchant that solicits, receives, and transmits payment card information on its checkout webpage, Savory must comply with security measures of applicable payment card brands. These security measures are derived from the Payment Card Industry's Data Security Standard.

12. Sometime between April 2018 and September 17, 2020, an unknown criminal accessed Savory's webserver and modified a JavaScript file used to transmit customer payment card information from Savory's checkout webpage to its third-party payment card processor. The criminal changed the file to copy and send the card information to a remote server at the same time the file sent the information to the payment card processor.

13. On September 17, 2020, the payment card processor told Savory that many payment cards used to purchase items on Savory's website were compromised and its website was likely insecure. Within hours, Savory found and deleted a malicious file located on its website.

14. On November 5, 2020, Savory's third-party forensic investigator concluded that the criminal used the malicious file to monitor and steal customer payment card information entered into Savory's checkout webpage. The investigator was unable to determine the date or method of the intrusion.

15. Upon concluding its investigation, the investigator recommended four PCI DSS security requirements for savory to implement: 1) preserve all webserver logs, 2) implement checksum software that fingerprints all webserver files and alerts Savory to unauthorized changes, 3) deploy an intrusion detection system, and 4) implement a web application firewall.

16. Though Savory was aware that customer information had been compromised, Savory did not start its consumer notification process until two months later in January 2021.

17. Savory installed a file checksum software in February 2021.

18. On March 27, 2021, Savory discovered a second, independent attack on its webserver. Though Savory was prepared to send consumer notices regarding the first data breach at this time, it chose to not to send notice until it completed a full investigation into this second attack.

19. On July 15, 2021, Savory's investigation into the second attack determined that a criminal monitored and stole customer payment card information for several hours on March 27.

20. On July 23, 2021, Savory mailed written notice to consumers that conducted an online transaction on Savory's website between April 2018 to October 8, 2020 or on March 27, 2021.

21. Savory implemented a web application firewall in May 2021.

22. At the time of the first breach, Savory's online privacy policy promised customers that "[s]hould a data breach occur, we will notify you via email within 30 days."

23. At the time of the first breach, Savory employed some technical safeguards to secure its website, but did not maintain any written security policies except for an acceptable use policy in its Employee Handbook.

24. Savory created an Emergency Management Plan in September 2021 and implemented a Document Retention Policy in October 2021. To date, Savory has not created an information security policy.

C. <u>Legal Allegations.</u>

1. Savory failed to timely notify impacted Colorado residents.

25. Savory maintained PII of its customers, namely payment card information.

26. When Savory determined that its customers' payment card information was compromised, it was required to send notice to impacted Colorado residents within 30 days.

27. Savory obtained clear information that its website was compromised in mid-September 2020, then conducted an eight-week security breach investigation. Savory notified impacted Coloradans 131 days after concluding its investigation—101 days after the timeframe contemplated by C.R.S. section 6-1-716.

2. Savory failed to comply with Colorado's Data Protection Statute.

28. Under C.R.S. section 6-1-713.5, Savory was required to implement reasonable security procedures and practices because it maintained PII of its customers.

29. A company of Savory's size that maintains customer information must take a comprehensive approach to data security, but Savory failed to do so.

30. Before the first breach, Savory failed to implement reasonable security measures including administrative safeguards such as an information security policy and incident response plan and technical measures including a web application firewall, checksum software, an intrusion detection system, and long-term webserver log storage.

31. Savory took an unreasonable amount of time remediating and implementing administrative safeguards. Savory took months to adopt its investigator's security recommendations—not implementing some until after it fell victim to a second payment card skimming attack.

32. Savory did not create an incident response plan until September 2021, a year after discovering the first breach.

33. As of June 13, Savory has not implemented an information security policy.

3. Savory failed to comply with Colorado's Data Disposal Statute.

34. Savory did not have a written information disposal policy as required by C.R.S. section 6-1-713 until October 2021.

35. Each of Savory's violations of C.R.S. sections 6-1-713, 6-1-713.5, and 6-1-716 constituted a deceptive trade practice under the CCPA. C.R.S. § 6-1-105(1)(x).

V. LEGAL AUTHORITY

36. C.R.S. section 6-1-110(2) authorizes the Attorney General to accept an assurance of discontinuance of any deceptive trade practice listed in Part 7 of the CCPA. Section 6-1-110(2) also allows the Attorney General to accept a voluntary payment from Savory of the costs of the State's investigation and any action or proceeding by the Attorney General.

VI. CONSIDERATION

37. The Parties enter into this Assurance for the purpose of compromising and resolving all disputed claims and to avoid further expense of protracted litigation. This Assurance does not constitute an abandonment by the State of its claim that Savory has violated the CCPA.

38. Savory shall pay to the State $40,000. Within 10 days of the Effective Date, Savory will pay $30,000 to the State. The State agrees to suspend Savory's payment of the remaining $10,000 if Savory complies fully with the terms outlined in paragraphs 39 through 46. The State acknowledges that Savory has already undertaken or completed some of the terms outlined in paragraphs 39 through 46 as of the date of this Assurance. Payment shall be in the form of a certified check, cashier's check, or money order made payable to the "Colorado Department of Law," shall reference "In the Matter of Savory Spice Shop, LLC" and shall be delivered to:

Emily Lujan, Administrative Assistant
Consumer Protection section
Colorado Department of Law
1300 Broadway, 7th Floor
Denver, Colorado 80203

All payments under this paragraph 38 are to be held, along with any interest thereon, in trust by the Attorney General to be used in the Attorney General's sole discretion for reimbursement of the State's actual costs and attorneys' fees, the payment of restitution, if any, and for future consumer fraud or antitrust enforcement, consumer education, or public welfare purposes.

VII. FURTHER ASSURANCES OF SAVORY

39. Savory, and any of its principals, officers, directors, agents, employees, representatives, successors, affiliates, subsidiaries, contractors, and assigns who have received actual notice of this Assurance, agree that:

A. Information Security Requirements.

40. Within 90 days after the Effective Date, Savory shall comply with the provisions of C.R.S. section 6-1-713.5.

41. As part of Savory's compliance with this Assurance, within 90 days after the Effective Date, Savory shall develop, implement, and maintain a comprehensive written information security program (WISP) reasonably designed to protect the security, integrity, and confidentiality of PII. The WISP shall describe how it complies with the requirements of Colorado law, adheres to an Appropriate Standard for the protection of PII, and contains administrative, technical, and physical safeguards appropriate to:

a. The size and complexity of Savory's operations;

b. The nature and scope of Savory's activities; and

c. The sensitivity of the PII that Savory maintains, licenses, or owns.

42. The WISP shall address the specific vulnerabilities leading to the breach, including:

a. A designated employee to develop and implement the information security program;

b. Written policies that adhere to an Appropriate Standard for the secure online collection and transmission of payment card information;

c. Save all logs from the webserver and the operating systems for as long as practicable;

d. Use a log management tool to timely identify unauthorized login activity;

e. Deploy a tool that checksums every file on Savory's system and alerts Savory to unauthorized file changes in real time;

f. Employ an intrusion detection system for Savory's network; and

g. Run Savory's website behind a web application firewall.

43. Savory shall, on at least an annual basis, conduct a comprehensive review of the safeguards it has put in place to protect PII so that Savory is up to date with any modifications to the Appropriate Standard.

B. <u>Incident Response and Breach Notification Requirements.</u>

44. Savory shall comply with the provisions of C.R.S. section 6-1-716 by creating an Incident Response Plan ("Plan") within 30 days after the Effective Date. The plan will include:

a. A designated employee responsible for developing and implementing the Plan;

b. Creation of an incident response team; and

c. A requirement that the incident response team establish milestones designating when the company will accomplish specific tasks to ensure that Savory complies with the requirements of C.R.S. section 6-1-716. On the date of each milestone, the company's incident response team must submit a written status report to Savory's leadership, including the president, detailing steps taken in the investigation to accomplish the given tasks.

45. Savory shall submit compliance reports, sworn under penalty of perjury by an individual or individuals with authority to bind Savory, to the Attorney General on the first and third anniversaries of the Effective Date of this Assurance. The compliance reports must:

a. Identify the primary postal and email address and telephone number, as designated points of contact, which the State may use to communicate with Savory in connection with this Assurance;

b. Describe, in detail, the steps Savory has taken to comply with each paragraph of this section VII;

c. Identify and describe all data security incidents or potential data security incidents that have occurred in the reporting period,

including a detailed description of all steps taken in any investigations Savory has undertaken; and

d. Describe all adjustments or improvements Savory has made as a result of any security incident or potential data security incident reported under paragraph 45(c), above.

46. Savory further agrees to cooperate with any proceedings or investigations arising out of the State's monitoring or investigation of Savory's compliance with this Assurance. This includes submission of additional compliance reports the State may reasonably request, promptly responding to reasonable requests for information made by the State and accepting service of Civil Investigative Demands.

VIII. RELEASE

47. The State acknowledges by its execution hereof that this Assurance constitutes a complete settlement and release of all claims under the CCPA on behalf of the State against Savory with respect to all claims, causes of action, damages, fines, costs, and penalties which were asserted or could have been asserted under the CCPA for the conduct described in this Assurance, that arose prior to the Effective Date and relating to or based upon the acts or practices which are the subject of this Assurance. The State agrees that, except as provided in the following paragraph, it shall not proceed with or institute any civil action or proceeding under the CCPA against Savory for any conduct or practice prior to the Effective Date which relates to the subject matter of this Assurance.

48. Nothing herein precludes the State from enforcing this Assurance, or from pursuing any law enforcement action under the CCPA with respect to the acts or practices of Savory not covered by this Assurance or any acts or practices of Savory conducted after the Effective Date. Nothing herein shall be construed to be a waiver or limitation of Savory's legal rights, remedies, or defenses in connection with any claim, matter, or suit related to the subject matter of this Assurance other than an action by the State to enforce the provisions of this Assurance.

IX. ENFORCEMENT

49. The obligations set forth in this Assurance are continuing.

50. The Parties consent to venue and jurisdiction for any proceeding necessary to enforce the terms of this Assurance within the District Court, Denver County, Colorado.

51. A violation of any of the terms of this Assurance shall constitute a prima facie violation of the CCPA under C.R.S. section 6-1-110(2). If the State believes that Savory has violated any term of this Assurance, the State shall be entitled to file a civil action under the CCPA and to seek an injunction or other appropriate order from such court to enforce the provisions of this Assurance.

52. In any such action, upon a showing by the State of a material violation of this Assurance by Savory, Savory stipulates to 1) a judgment in the amount of $10,000, which reflects the suspended payment described in ¶ 38, above; and 2) an order converting this Assurance into a permanent injunction against Savory. The State may seek, and the Court may enter, any additional remedies, including but not limited to additional monetary remedies, that are deemed proper. Savory agrees to waive any counterclaims that it may have had with respect to the subject matter of this Assurance and agrees to limit any defenses to (1) whether a violation has occurred; and (2) the remedies for the violation.

X. MISCELLANEOUS PROVISIONS

53. This Assurance is the final, complete, and exclusive statement of the Parties' agreement on the matters contained herein, and it supersedes, terminates, and replaces any and all previous negotiations, agreements, and instruments as may exist between the Parties. Other than any representation expressly stated in this Assurance, the Parties have not made any representations or warranties to each other, and no Party's decision to enter into this Assurance is based upon any statements by any other Party outside of those in this Assurance. No change or modification of this Assurance shall be valid unless in writing and signed by all Parties. If any provision(s) of this Assurance is held to be invalid, illegal, or unenforceable, the validity, legality, and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.

54. This Assurance shall neither create nor waive or otherwise affect any private rights or remedies in any third parties nor waive any rights, remedies, or defenses of the Parties in respect to any third parties. Under no circumstances shall this Assurance or the name of the Attorney General or any of the State's employees or representatives be used by Savory or any person under their direction or control to suggest the State's endorsement of Savory's past, present, or future conduct.

55. Nothing herein relieves Savory of its duty to comply with all applicable laws, regulations, or rules of the State of Colorado nor constitutes authorization by the State for Savory to engage in acts and practices prohibited by such laws.

56. Savory acknowledges that it is the State's customary position that an agreement restraining certain conduct by a party does not prevent the State from addressing later conduct that could have been prohibited, but was not, in the earlier agreement, unless the earlier agreement expressly limited the State's enforcement options in that manner. Therefore, nothing herein shall be interpreted to prevent the State from taking enforcement action to address conduct occurring after the Effective Date that the State believes to be in violation of the law. The fact that such conduct was not expressly prohibited by the terms of this Assurance shall not be a defense to any such enforcement action.

57. The terms and provisions of this Assurance may be enforced by the current Colorado Attorney General, and by any of his duly authorized agents or representatives, as well as by any of his successors in interest, and by any of his successors in interest's agents or representatives.

58. Pursuant to C.R.S. section 6-1-110(2), this Assurance shall be a matter of public record.

59. Savory acknowledges that it had a full opportunity to review this Assurance and consult with legal counsel regarding it. The undersigned

representatives of Savory agree and represent that they have read and understood this Assurance, accept the legal consequences involved in signing it, and that there are no other representations, agreements, or understandings between the State and Savory that are not stated in writing herein.

60. This Assurance may be signed in one or more counterparts, each of which shall be deemed an original, but which together shall constitute the Assurance. Electronic copies of this Assurance and the signatures hereto may be used with the same force and effect as an original.

XI. Notice

61. All notices regarding this Assurance shall be sent by certified mail, return receipt requested or reputable overnight delivery service (e.g., FedEx, UPS) at the addresses set forth below unless any Party notifies the other Parties in writing of another address to which notices should be provided:

If to Savory Spice Shop, LLC.:

Janet C. Johnston
Savory Spice Shop, LLC
1805 E. 58th Ave., Unit C
Denver, Colorado 80216
jjohnston@savoryspiceshop.com

With copies to legal counsel by Regular U.S. Mail and e-mail:

Michael E. Lindsay
Ellie Lockwood
Snell & Wilmer LLP
1200 17th Street, Suite 1900
Denver, CO 80202
mlindsay@swlaw.com
elockwood@swlaw.com

If to the State:

Colorado Attorney General
1300 Broadway, 7th Floor
Denver, Colorado 80203
Attn.: Abigail Hinchcliff, First Assistant Attorney General,
abigailhinchliff@coag.gov
Attn: Mark Bailey, Senior Assistant Attorney General II, mark.bailey@coag.gov
Attn: Chelsea Kelleher, Assistant Attorney General, chelsea.kelleher@coag.gov

[Signatures appear on the following page(s)]

STATE OF COLORADO:

PHILIP J. WEISER,
ATTORNEY GENERAL

By:

s/ Chelsea Kelleher

Chelsea A. Kelleher
Assistant Attorney General
Attorney Reg. No. 55041

SAVORY SPICE SHOP, LLC.

By:

Janet C. Johnston, President

s/Ellie Lockwood

Ellie Lockwood
Counsel for Savory
Atty. Reg. No. 43271