STATE OF COLORADO
DEPARTMENT OF LAW

ASSURANCE OF DISCONTINUANCE

IN THE MATTER OF SEMA CONSTRUCTION, INC.

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 SEMA Construction, Inc. ("SEMA") 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 SEMA (the "Parties") regarding the State's allegations as to the security breach that SEMA first detected on September 7, 2019.

I. INTRODUCTION

Cybercrime and identity theft threaten the wellbeing of Colorado residents. A prevalent example of a cybercrime is phishing, where a criminal sends fraudulent emails to obtain login credentials and gain unauthorized access to email accounts. A successful phishing attack harms individuals when a criminal uses stolen information to commit or allow others to commit identity theft. Businesses play an integral role in thwarting phishing scams and protecting individuals' information when they implement proper technical safeguards and train their employees to detect phishing and other similar scams.

Colorado law requires companies that maintain sensitive personal information to take reasonable steps to protect the information, to dispose of it when it is no longer

needed, and to notify Colorado residents promptly when their information is at risk of being misused by unauthorized third parties.

SEMA is based in Centennial, Colorado and operates construction sites throughout the United States. SEMA maintained sensitive personal information of Colorado residents, including social security numbers and financial information. SEMA allowed some of this information to be stored in employee email accounts and failed to dispose of it long after it was needed.

SEMA was the victim of a phishing attack in which a criminal gained access to login credentials for the email accounts of multiple SEMA employees. This attack exposed the confidential information that was stored in the employees' email accounts. SEMA's inadequate data security practices allowed a cybercriminal to access SEMA's emails, including those containing personal information of Colorado residents, for eleven months before SEMA detected the intrusion.

Due to SEMA's unreasonably long investigation and delayed notice, affected Coloradans were unaware that their information had been compromised until 16 months after SEMA discovered the breach. The Parties enter into this Assurance to ensure SEMA'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. SEMA is a Colorado corporation with a principal office address of 7353 S. Eagle Street, Centennial, CO 80112.

III. DEFINITIONS

3. The term "Appropriate Standard" means a cybersecurity standard or controls set by 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.* § 6-1-716(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. SEMA maintains, owns, or licenses PII, including social security numbers, bank account and routing numbers, passport information, driver's license numbers, and medical information of SEMA's employees, their dependents, and job applicants.

11. SEMA employees are allowed to send PII to authorized individuals and receive PII through email. At the time of the breach, SEMA allowed employees to store PII in their email accounts.

12. Starting on October 15, 2018, an unknown criminal targeted SEMA employees in a phishing campaign.

13. SEMA discovered an intrusion to employee email accounts on September 7, 2019, when a compromised employee email account sent phishing emails to other employees. SEMA started an investigation the same day.

14. On September 30, SEMA retained lawyers to assist in the investigation. SEMA's lawyers retained a third-party forensic data investigation firm in October to determine the scope of the incident, including whether the criminal accessed PII.

15. The forensic investigators issued a report to SEMA on December 2, 2019. The report found that the criminal used employee login credentials to obtain unauthorized access to four employee email accounts and recommended that SEMA identify potentially impacted individuals. SEMA requested a quote from the firm to conduct this review.

16. SEMA's investigation into the security breach did not progress from mid-January 2020 to May 28, 2020 due to communication issues between SEMA and its lawyers. On June 9, SEMA retained another forensic data analysis firm to review the contents of the compromised accounts for personal information. The total volume of the data reviewed was 26.36 GB.

17. On August 4, the firm informed SEMA that the criminal had access to the PII in the accounts. The firm issued its formal report on August 6 detailing the results from the programmatic and manual review of the impacted information. SEMA informed the Attorney General that "[o]n August 20, 2020, [SEMA] . . . received detailed information indicating that PII records had been compromised through the email incident."

18. The affected PII included names, social security numbers, bank account and routing numbers, passport information, driver's license numbers, and medical information.

19. On August 21, 2020, SEMA identified 1,289 Colorado employees that may have been affected by the breach. SEMA provided notice to these employees on October 1, 2020.

20. On December 4, 2020, SEMA identified an additional 662 impacted Colorado residents. SEMA sent notice to these residents on December 30, 131 days after learning PII had been compromised.

21. At the time of the breach, SEMA had some technical safeguards to secure its systems and email environment. This included following Microsoft 365's password policy, employing malicious email filtering and email archiving, and using multi-factor authentication for system administrators. SEMA's only written data protection policy was found in its Information Technology Manual, which prohibited employees from sharing sensitive information with unauthorized parties.

22. At the time of the breach, SEMA did not have a data disposal policy. After conducting a review of the affected email accounts, SEMA determined that the oldest email found in the compromised email accounts was dated October 2, 2001. SEMA informed the Attorney General that it is confident all persons with affected PII were notified. However, SEMA's investigation was not able to determine the date of the oldest email in the affected accounts that contained PII.

23. SEMA did not provide cybersecurity training to its employees prior to the breach. SEMA first provided cybersecurity training to its Information Technology employees in April 2020, eight months after discovering the intrusion. As of June 8, 2021, some employees had not completed training assigned in February 2021.

24. SEMA made some efforts to improve its cybersecurity after discovering the intrusion. This included implementing additional technical safeguards for its email environment and creating a Password Policy and an Acceptable Use Policy.

25. After the State requested information from SEMA about its security practices, SEMA adopted several security policies around May 28, 2021 including a data disposal policy, a comprehensive sensitive information policy, and an incident response plan.

C. Legal Allegations.

1. SEMA failed to comply with Colorado's Data Disposal Statute.

26. SEMA maintained PII of its employees, their dependents, and job applicants in paper and computerized form.

27. SEMA did not have an information disposal policy as required by C.R.S. Section 6-1-713 until May 28, 2021. This failure allowed the cybercriminal to access PII that accumulated in employee mailboxes for up to twenty years.

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

28. Under C.R.S. Section 6-1-713.5, SEMA was required to implement reasonable security procedures and practices because it maintained PII of its employees, their dependents, and job applicants.

29. A company of SEMA's size that maintains the kinds of PII that SEMA does must take a comprehensive approach to data security, but SEMA failed to do so.

30. Employees of SEMA sent PII in emails and stored emails containing PII in their mailboxes for up to twenty years. SEMA failed to provide cybersecurity training, including phishing detection training, to its employees and properly dispose of and secure stored PII. This left PII vulnerable to phishing and other compromises.

31. SEMA failed to assess its cybersecurity risks and failed to implement appropriate comprehensive security policies to mitigate or eliminate those risks even after the breach alerted SEMA to deficiencies in its security practices and incident response preparedness.

3. SEMA failed to comply with Colorado's Security Breach Statute in two ways.

a. SEMA failed to conduct a prompt, good faith investigation.

32. When SEMA discovered that employee email accounts were compromised, it was required to undertake a prompt, good faith investigation to determine whether a security breach occurred. C.R.S. § 6-1-716(2)

33. SEMA took 11 months to complete its investigation of the security breach, including a five-month period where no progress toward identifying and notifying affected individuals was made.

34. SEMA did not have an incident response plan at the time of the breach, which left it ill-prepared to take the steps required to provide timely notice.

b. SEMA failed to timely notify impacted Colorado residents.

35. SEMA notified one group of impacted Colorado residents on October 1, 2020, 42 days after concluding its security breach investigation.

36. SEMA notified a second group of impacted Colorado residents on December 30, 2020, 131 days after concluding its security breach investigation – and 16 months after SEMA discovered the intrusion.

37. Each of SEMA'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

38. 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 SEMA of the costs of the State's investigation and any action or proceeding by the Attorney General.

VI. CONSIDERATION

39. 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 admission by SEMA of any violation of the CCPA, nor shall it be construed as an abandonment by the State of its claim that SEMA has violated the CCPA.

40. SEMA shall pay to the State $80,000 and the State's attorneys' fees of $8,242.12. Within 10 days of the Effective Date, SEMA will pay $63,242.12 to the State. The State agrees to suspend SEMA's payment of the remaining $25,000 if SEMA complies fully with the terms outlined in paragraphs 41 through 49. The State acknowledges that SEMA has already undertaken or completed some of the terms outlined in paragraphs 41 through 49 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 SEMA Construction, Inc." and shall be delivered to:

Ruth Seminara, Administrative Assistant
Consumer Protection Section
Colorado Department of Law
1300 Broadway, 7th Floor
Denver, Colorado 80203

All payments under this paragraph 40 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 SEMA

41. SEMA, 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. Data Disposal Requirements.

42. Within 30 days of the Effective Date, SEMA shall develop and implement a written policy for the destruction or proper disposal of paper and electronic documents containing PII that complies with C.R.S. Section 6-1-713.

B. Information Security Requirements.

43. Within 90 days after the Effective Date, SEMA shall comply with the provisions of C.R.S. Section 6-1-713.5.

44. As part of SEMA's compliance with this Assurance, within 90 days after the Effective Date, SEMA shall develop, implement, and maintain a comprehensive

written information security program (ISP) reasonably designed to protect the security, integrity, and confidentiality of PII. The ISP 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 SEMA's operations;

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

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

45. The ISP 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 storage and proper disposal of PII;

c. At least annual training on secure storage and handling of PII that includes but is not limited to phishing awareness and detection for all employees and other workers;

d. Appropriate controls to verify user identity upon system or application access with supporting rationale; and

e. Policies and protocols for employee reporting of suspected phishing emails and prompt institutional response.

46. SEMA shall, on at least an annual basis, review the safeguards it has put in place to protect PII so that SEMA is up to date with any modifications to the Appropriate Standard.

C. Incident Response and Breach Notification Requirements.

47. SEMA 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 SEMA 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 SEMA's leadership, including the president, detailing steps taken in the investigation to accomplish the given tasks.

48. SEMA shall submit compliance reports, sworn under penalty of perjury by an individual or individuals with authority to bind SEMA, 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 SEMA in connection with this Assurance;

b. Describe, in detail, the steps SEMA 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 SEMA has undertaken; and

d. Describe all adjustments or improvements SEMA has made as a result of any security incident or potential data security incident reported under paragraph 48(c), above.

49. SEMA further agrees to cooperate with any proceedings or investigations arising out of the State's monitoring or investigation of SEMA'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

50. 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 SEMA 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 SEMA for any conduct or practice prior to the Effective Date which relates to the subject matter of this Assurance.

51. 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 SEMA not covered by this Assurance or any acts or practices of SEMA conducted after the Effective Date. Nothing herein shall be construed to be a waiver or limitation of SEMA'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

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

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

54. 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 SEMA 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.

55. In any such action, upon a showing by the State of a material violation of this Assurance by SEMA, SEMA stipulates to 1) a judgment in the amount of $25,000, which reflects the suspended payment described in ¶ 40, above; and 2) an order converting this Assurance into a permanent injunction against SEMA. The State may seek, and the Court may enter, any additional remedies, including but not limited to additional monetary remedies, that are deemed proper. SEMA 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; (2) the remedies for the violation.

X. MISCELLANEOUS PROVISIONS

56. 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.

57. 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 SEMA or any person under their direction or control to suggest the State's endorsement of SEMA's past, present, or future conduct.

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

59. SEMA 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.

60. 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.

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

62. SEMA acknowledges that it had a full opportunity to review this Assurance and consult with legal counsel regarding it. The undersigned representatives of SEMA 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 SEMA that are not stated in writing herein.

63. 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

64. 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 SEMA Construction, Inc.

Steve Hathaway (shathaway@sema.inc)
Matt Mosley (mmosley@sema.inc)
Josh Clyne (jclyne@sema.inc)
Matt Donars (mdonars@sema.inc)
SEMA Construction, Inc.
7353 S. Eagle St., Centennial, CO 80112

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

James Monagle
Mullen Coughlin LLC
309 Fellowship Rd Suite 200
Mt. Laurel, NJ 08054
jmonagle@mullen.law

Amanda Harvey
Mullen Coughlin LLC
1452 Hughes Rd Suite 200
Grapevine, TX 76051
aharvey@mullen.law

If to the State:

Colorado Attorney General
1300 Broadway, 7th Floor
Denver, Colorado 80203
Attn.: Abigail Hinchcliff, First Assistant Attorney General,
abigail.hinchcliff@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

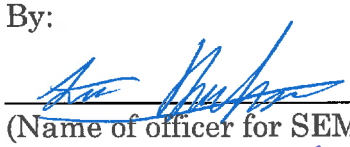
By:

s/ Chelsea Kelleher

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

SEMA CONSTRUCTION, INC.

By:



(Name of officer for SEMA)
Steve Hathaway (CFO/CIO)

s/James Monagle

(name of attorney), Counsel for SEMA – ######.