IN THE CIRCUIT COURT OF THE STATE OF OREGON

FOR THE COUNTY OF MULTNOMAH

IN THE MATTER OF: GUSTAFSON & COMPANY, LLC, an Oregon limited liability, Respondent.	Case No. ASSURANCE OF VOLUNTARY COMPLIANCE **ORS 20.140 - State fees deferred at filing**

INTRODUCTION

1.

This Assurance of Voluntary Compliance ("AVC") is entered into by the Attorney General of the State of Oregon, Ellen F. Rosenblum, and Gustafson & Company, LLC ("Gustafson"), an accounting firm based in Portland, Oregon, to resolve the Attorney General's investigation into a breach of security affecting personal information of consumers.

2.

The Oregon Department of Justice ("Oregon DOJ") submits this AVC to the Circuit Court of the State of Oregon in Multnomah County ("Court") for approval pursuant to ORS 646.632(2)

3.

Gustafson waives receipt of a Notice from the State of Oregon, pursuant to ORS 646.632(2).

4.

Gustafson understands and agrees this AVC applies to Gustafson, Gustafson's members, officers, agents, employees, representatives, successors and assigns, jointly and severally, while

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

acting personally, or through any corporation or other business entities, whose acts, practices or policies are directed, formulated or controlled by Gustafson.

5.

Gustafson understands and agrees that any notices or other documents required to be sent under this AVC shall be sent to the following address via first class and electronic mail. Any party may update its designee or address by sending written notice to the other party informing them of the change.

For Gustafson:

Charles J. Paternoster
Parsons, Farnell & Grein
1030 SW Morrison St.
Portland, OR 97205

For Oregon DOJ:

Kristen G. Hilton
Assistant Attorney General, Consumer Protection Section
1162 Court Street NE
Salem, OR 97301-4096

6.

Gustafson agrees to accept service of a conformed or court-certified copy by of this AVC by First-Class Mail sent to the addresses following Gustafson's signature, but otherwise waives any further notice of submission to and filing with the court of this AVC.

7.

Gustafson shall not represent to any third party that Oregon DOJ acquiesces or approves of Gustafson's past business practices, current efforts to reform their practices, or any future practices, which they may adopt or consider adopting. Oregon DOJ's decision to settle this matter or to otherwise unilaterally limit current or future enforcement action does not constitute approval or imply authorization for any past, present, or future business practice.

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

8.

This AVC provides for the payment of an amount of money. If any payment is not paid within 30 days of the date specified herein, then Oregon DOJ may submit that portion of the AVC which provides for the payment of money to the Court with a certificate stating the unpaid balance in a form which fully complies with the requirements of ORS 18.038 and 18.042. Upon such submission under ORS 646.632(2), and upon signature by the Court, it shall be entered in the register of the Court and the clerk of the Court shall note in the register that it creates a lien. The AVC shall thereupon constitute a judgment in favor of the State of Oregon and may be enforced as provided in ORS chapter 18.

9.

Gustafson understands that violation of any of the terms of the AVC may result in contempt of court proceedings, a civil penalty of up to $25,000 per violation, and such further relief as the court may deem appropriate. See ORS 646.632(4), ORS 646.642(1) and ORS 646.642(2).

10.

This AVC is a settlement of disputed matters between the parties. Although Gustafson denies that it has engaged in unlawful or otherwise inappropriate business practices, Gustafson agrees to this AVC so that this matter may be resolved amicably, without further cost or inconvenience to the State of Oregon, its citizens or to Gustafson. In accordance with ORS 646.632(2), this AVC shall not be considered an admission of violation of law by Gustafson for any purpose.

FINDINGS

11.

On or about January 21, 2020, a threat actor posing as a client sent a malicious zip file containing a remote access trojan to Gustafson via email. At the time, Gustafson had firewalls and password protection in place, and anti-malware installed on its computer network, and had provided staff with some training. Gustafson responded to the email by providing a ShareFile link

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

for use in uploading the documents contained in the zip file, but did not first verify the validity of the sender's email address or scan the zip file for viruses or malware. A malicious W-2, sent via the ShareFile link, was uploaded to Gustafson's computer network, after a Gustafson employee clicked on a pop-up window in the document, which deployed a remote access trojan. The remote access trojan gave the threat actor access to a share drive containing encrypted 2018 tax return and other documents containing personal information for Gustafson's clients, including name, address, social security number, date of birth, and financial account numbers.

12.

On January 28, 2020, a bi-weekly Webroot scan of the Gustafson computer network by its outside IT vendor identified the potential malware and Gustafson's IT vendor removed it. The IT vendor also took the machine offline, performed a review, and wiped that PC before reconnecting it to the Gustafson network. The IT vendor did not identify whether any files had been accessed or exfiltrated through the remote access trojan.

13.

In February 2020, Gustafson learned that three clients had fraudulent 2019 tax returns filed. On March 5, 2020, Gustafson learned that five additional clients had fraudulent 2019 tax returns filed. At that time, Gustafson called their insurance company and hired a forensic investigation firm. That firm identified additional evidence that the January review failed to uncover, and they determined that from at least January 22, 2020 through January 28, 2020, the threat actor had used the remote access trojan to access some of the 2018 client tax return files contained on Gustafson's network share drive. Because of the nature of the remote access trojan, the threat actor was able to decrypt the files on the share drive.

14.

Gustafson represents that on April 10, 2020, it received verification of the breach from forensic investigator, SpearTip, Inc. Starting on May 21, 2020, Gustafson notified by letter the 2,207 consumers, including 1,881 Oregon consumers, whose information had been potentially

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

accessed and potentially acquired by the threat actor. Gustafson also submitted a data breach notification to Oregon DOJ.

15.

Gustafson represents that it provided one year of credit monitoring and theft resolution services at no charge to consumers potentially affected by the incident via Experian's IdentityWorks product. The product includes up to $1 million in identity theft insurance and is underwritten by insurance company subsidiaries or affiliates of AIG.

16.

Gustafson also represents that it worked with, and continues to work with, the IRS and ODR to assist consumers that had fraudulent returns as well as other consumers who may have been affected by the breach. Specifically, Gustafson represents that it is participating in the IRS Returns Inventory & Classification (RICS) system and Gustafson had all clients automatically enrolled in the IRS voluntary identity theft program, which provides consumers with unique pins to be used when filing 2020 tax returns.

17.

Oregon DOJ contends that Gustafson violated the Oregon Consumer Information Protection Act, ORS 646A.600-628, and Oregon Unlawful Trade Practices Act, ORS 646.605-656, by failing to have appropriate administrative and technical safeguards in place to prevent and timely mitigate/remediate the data breach, and by failing to timely notify consumers. Gustafson disputes that its conduct was in violation of any statute, law or administrative regulation.

DEFINITIONS

18.

For the purposes of this AVC, the following definitions shall apply:

(a) "Breach Notification Act" shall mean the Oregon Consumer Information Protection Act, ORS 646A.600-628.

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

(b) "Data Breach" shall mean the data security incident reported by Gustafson on May 21, 2020, in which a person or persons gained unauthorized access to portions of its computer network that stored consumer information;

(c) "Consumer" shall mean an individual resident of Oregon;

(d) "Network" shall mean all networking equipment, databases or data stores, applications, servers and endpoints that are capable of using and sharing software, data and hardware resources, and that are owned, operated, and/or controlled by Gustafson;

(e) "Personal Information" shall mean the data elements in the definition of personal information as set forth in ORS 646A.602; and

(f) "Security Event" shall mean any compromise that results in the unauthorized access, acquisition, or exfiltration of Personal Information owned, licensed, stored, or maintained by Gustafson; and

(g) "Vendor" shall mean a third party with which Gustafson contracts to provide services related to information technology, information security, cybersecurity or other similar support of computer-based systems.

ASSURANCES

19.

Gustafson shall comply with the Oregon Unlawful Trade Practices Act, ORS 646.605-656, and the Oregon Consumer Information Protection Act, ORS 646A.600-628.

20.

If Gustafson is subject to a breach of security or receives notice of a breach of security from a vendor, Gustafson shall give notice of the breach of security to: (a) the consumer to whom the personal information pertains, and (b) the Attorney General, either in writing or electronically, if the number of consumers to whom the covered entity must send the notice if it exceeds 250. ORS 646A.604(1). Gustafson shall give the notice in the most expeditious manner possible,

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security. ORS 646A.604(3)(a).

21.

Upon execution of this AVC, Gustafson agrees to adhere to each of the following requirements:

(a) Gustafson will develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of all Personal Information Gustafson has in its possession;

(b) Gustafson will develop, implement and maintain a breach response and notification plan that includes at least the following:

(1) Identification of the types of incidents that fall within the scope of the plan;

(2) A description of all individuals' roles in fulfilling responsibilities under the plan, including back-up contacts and escalation pathways;

(3) Regular testing and review of the plan. Based on the testing and review, Gustafson shall re-evaluate the plan and revise it, as is prudent or necessary;

(4) A requirement that Gustafson investigate all data security incidents. If a data security incident is determined to be a Security Event, Gustafson shall submit information regarding the incident to its insurer or, if no insurer, to its attorney, which shall review the incident and decide whether notification is required under applicable law, including the applicable version of the Breach Notification Act then in effect, which shall be documented in writing and communicated to Gustafson; and a

(5) A report that includes a description of any security incident that does not trigger notice under the Breach Notification Act, Gustafson's response to the security incident and why Gustafson determined that the security incident did not trigger notice under the Breach Notification Act. Gustafson must retain the report for two (2) years and make the report available to the Oregon DOJ upon request.

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

(c) Gustafson will develop, implement and maintain a comprehensive information security program. Within ninety (90) days of the execution of this AVC, Gustafson will adopt, update, implement, and maintain a comprehensive written information security program ("Information Security Program") that include at least the following:

(1) Data Security Plan: A written policy that includes administrative safeguards, technical safeguards and physical safeguards which are appropriate based on the size and complexity of Gustafson's operations, the nature and scope of Gustafson's activities and the sensitivity of the personal information that Gustafson maintains or otherwise possesses;

(2) Designated Individual: An employee or contractor with appropriate background or experience in information security who is responsible for implementing and maintaining the information security program and advising appropriate personnel of Gustafson's security posture, security risks faced by Gustafson and security implementations of Gustafson's decisions;

(3) Resources: Sufficient resources and support to reasonably ensure the functionality of the Information Security Program;

(4) Vendor Requirements: A list of the specific roles and responsibilities to be undertaken by Gustafson and by the Vendor in all Vendor contracts. To the extent that Gustafson "outsources" the technical work to be performed under the Information Security Program, Gustafson will ensure that its Vendor contract contains clear provisions if the Vendor will be providing services for network security, penetration testing, vulnerability testing, file integrity monitoring, or review of network logs. Gustafson will periodically review the Vendor's performance for compliance with the contract. Such periodic review will occur no less than one time per year.

(5) Monitoring Logs: Proactive regular monitoring of network firewall logs, including a real-time scanning solution designed to notify personnel of suspect activity to critical applications or operating system files on the Network. Gustafson shall ensure logging and

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

monitoring processes are executed, updated and maintained to ensure that firewall Network activity is adequately logged, that security incidents are regularly reviewed in near real-time, and that appropriate follow-up is taken;

(6) Privileged Account Management: A system to secure use of privileged credentials, such as through a privileged access management tool that vaults credentials and requires multifactor authentication or other greater method of control for access;

(7) Authentication:

a. Multifactor authentication for Gustafson's system administrator accounts and for all remote access to the Network;

b. Review and, as appropriate, restriction or disabling of unnecessary accounts on the Network. Gustafson shall ensure that local administrative accounts have unique passwords or other appropriate controls across the environment and multi-factor authentication for remotely connecting to the Network;

(8) Antivirus and Anti-malware Maintenance: The implementation and maintenance of current, up-to-date antivirus and anti-malware protection programs on Gustafson's computer systems. Such antivirus and anti-malware protection programs shall include screening of incoming emails and email attachments including .zip files.

(9) Employee Training: Training regarding phishing email attacks for employees that have access to any system that receives communications and information. Gustafson shall provide information about phishing attacks in its Employee Handbook, including what to do if an employee receives an email attachment from an outside source. Gustafson shall incorporate into its Employee Handbook a defined process for employees to report any concern about Gustafson's security systems, including the process for review of a concern, Gustafson's response to the concern, and whether and when Executive staff is informed of the concern;

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

(10) Encryption: Gustafson shall encrypt all records containing Personal Information, whether stored within the Network, or transmitted electronically within or outside the Network, using a reasonable encryption algorithm. Gustafson will update its encryption protocols as consistent with the evolution of technology and industry standards;

(11) Password Management: Gustafson shall implement and maintain reasonable password policies and procedures requiring the use of complex passwords, and ensuring that stored passwords are properly protected from unauthorized access, including, without limitation, hashing stored passwords using a reasonable hashing algorithm;

(12) Penetration Testing: Implementing and maintaining a risk-based penetration testing program reasonably designed to regularly identify, assess and remediate penetration vulnerabilities within Gustafson's Network; and

(13) Whitelisting: Deploying and maintaining controls designed to detect and prevent the execution of unauthorized applications within Gustafson's Network or the unauthorized exfiltration of information from Gustafson's Network.

22.

Gustafson may satisfy paragraph 21(a) through the review, maintenance and, if necessary, updating, of an existing information security program that complies with paragraph 21(c).

PAYMENT TO STATE

23.

Within sixty [60] days after entry of this AVC, Gustafson shall pay to Oregon DOJ the sum of fifty thousand dollars [$50,000] to be deposited into the Department of Justice account established pursuant to ORS 180.095 and used by Oregon DOJ as allowed by law. Payment shall be made by electronic transfer in accordance with instructions provided by Oregon DOJ.

///

///

///

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

RELEASE

24.

The parties acknowledge and agree that this AVC constitutes a full and final release by the Attorney General of Gustafson, Gustafson's members, officers, agents, employees, representatives, successors and assigns from any claims of the Attorney General under the Unlawful Trade Practices Act, ORS 646.605 to 646.656, relating to the Data Breach which occurred before the date of execution of this AVC. Gustafson agrees and understands that nothing in this AVC shall be construed to release or compromise any relief to which Oregon DOJ may be entitled by law or under this AVC as a result of Gustafson's failure to comply with any provision of this AVC.

MISCELLANEOUS PROVISIONS

25.

The parties acknowledge that no other promises, representations, or agreements of any nature have been made or entered into by the parties. The parties further acknowledge that this AVC constitutes a single and entire agreement that is not severable or divisible, except that if any provision herein is found to be legally insufficient or unenforceable, the remaining provisions shall continue in full force and effect.

APPROVAL BY COURT

APPROVED for filing and so ORDERED:

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

REVIEW BY GUSTAFSON'S ATTORNEY

Approved as to form. Dated Sept 9, 2021.

Attorney for Gustafson

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

GUSTAFSON'S SIGNATURE AND ACKNOWLEDGMENT

Gustafson has read and understands this agreement and each of its terms. Gustafson agrees to each and every term.

Corporate Gustafson

I, Kenneth E. Gustafson being first duly sworn on oath, depose and say that I am the managing member of GUSTAFSON AND COMPANY LLC and am fully authorized and empowered to sign this Assurance of Voluntary Compliance on behalf of GUSTAFSON AND COMPANY LLC and bind the same to the terms hereof.

Signature

Kenneth E. Gustafson
Print Name

Address 5200 S. Macadam Ave #470
Portland, Oregon 97239

SUBSCRIBED AND SWORN to before me this 16th day of September, 2021.

Notary Public for
My Commission Expires: 12/10/2021

OFFICIAL STAMP
JILL ANN BOBZIEN
NOTARY PUBLIC-OREGON
COMMISSION NO. 968680
MY COMMISSION EXPIRES DECEMBER 10, 2021

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

ACCEPTANCE OF DOJ

Accepted this 17th day of September, 2021.

ELLEN F. ROSENBLUM
Attorney General

Kristen G. Hilton, OSB #151950
Assistant Attorney General
Department of Justice
Of Attorneys for Plaintiff
Consumer Protection Section
1162 Court Street NE
Salem, OR 97301-4096
Phone: 503-934-4400
Fax: 503-378-5017
Email: kristen.hilton@doj.state.or.us

Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017

CERTIFICATE OF READINESS

This proposed ***Assurance of Voluntary Compliance*** is ready for judicial signature because:

1**. [X]** **Each opposing party affected by this order has stipulated to the order, as shown by each opposing party's signature on the document being submitted.**

2. [ ] Each opposing party affected by this order has approved the order, as shown by signature on the document being submitted or by written confirmation of approval sent to me.

3. [ ] I have served a copy of this order on all parties entitled to service and provided written notice, and:

a. [ ] No objection has been served on me.

b. [ ] I received objections that I could not resolve with the opposing party despite reasonable efforts to do so. I have filed with the court a copy of the objections I received and indicated which objections remain unresolved.

c. [ ] After conferring about objections, [role and name of opposing party] agreed to file any remaining objection with the court by [date], which predated my submission.

4. [ ] The relief sought is against an opposing party who has been found in default.

5. [ ] An order of default is being requested with this proposed judgment.

6. [ ] Service is not required by statute, rule, or otherwise.

DATED September 17, 2021.

KRISTIN G. HILTON, OSB#151950
Assistant Attorney General
Civil Enforcement Division
Oregon Department of Justice
Email: kristen.hilton@doj.state.or.us

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 934-4400 / Fax: (503) 378-5017