Baker McKenzie.

Baker & McKenzie LLP

Two Embarcadero Center, 11th Floor
San Francisco, CA 94111-3802
United States

Tel: +1 415 576 3000
Fax: +1 415 576 3099
www.bakermckenzie.com

CONFIDENTIAL

June 06, 2019

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street, Concord, NH 0330

By certified mail
Receipt / Delivery Details

Notice of Data Breach

Dear Mr. MacDonald,

I write on behalf of Avalara, Inc. ("**Avalara**") to notify you that Avalara recently learned about a vulnerability that resulted in the accidental exposure to a third party of certain personal information that Avalara received in connection with providing online services to its customers. These online services relate to a software application called eCompli which Avalara recently purchased from a company called Compli, Inc. The third party informed Avalara of the vulnerability after discovering it, and subsequently deleted all copies of personal information that they accessed via the vulnerability. The third party also certified that they did not share the personal information they accessed via the vulnerability with any other party. Avalara has taken reasonable and appropriate steps to address and remove the vulnerability, and its investigation indicated that this third party was the only party that accessed the personal information via the vulnerability.

In greater detail: On May 22, 2019, an employee of one of Avalara's customers (who happens to be a former employee of Compli, Inc.) notified Avalara that an eCompli code update contained a vulnerability that allowed the employee to gain unauthorized access to certain personal information about certain individuals at some of Avalara's customers. In particular, the vulnerability enabled the third party to potentially access these individuals' first and last names, organization, social security number, driver's license number and state, contact information, date and place of birth, citizenship status, eye and hair color, weight, height, marital status, marriage date and place, employment history, residence history and State Alcohol Board license number and date of expiration. This third party informed Avalara of the vulnerability and Avalara subsequently removed the vulnerability on May 22, 2019. The third party also certified that they did not share with any other party, and deleted all copies, of the information they accessed via the vulnerability.

In response to the notification from this third party, Avalara promptly conducted an investigation to determine the scope of the incident, confirmed that the vulnerability was removed on May 22, 2019, and took reasonable and appropriate steps to ensure that the security and integrity of eCompli has been restored. Avalara also confirmed by reviewing its

Baker McKenzie.

internal logs that this third party was the only entity who accessed personal information via the vulnerability. Avalara and its service providers have reviewed their security protocols and taken steps to address the security of the platform. Avalara and its service providers are closely monitoring eCompli to help protect against future unauthorized access.

Avalara is providing on June 6, 2019, postal mail notifications to impacted individuals, informing them of the incident, and encouraging them to take security precautions regarding their personal information. The number of affected data subjects in New Hampshire is 2.

Affected individuals may contact Avalara at 805-226-5350. We attach a copy of Avalara's sample data subject notice. Please feel free to contact me directly at 415-984-3883 or jonathan.tam@bakermckenzie.com.

Best regards,

Jonathan Tam
Attorney
415-984-3883
jonathan.tam@bakermckenzie.com

Avalara, Inc.
1650 Ramada Drive, Suite 180
Paso Robles, CA 93446

[*Date*]

[*Name of data subject*]
[*Address*]

NOTICE OF DATA BREACH

Thank you for being an eCompli user. Avalara, Inc., recently purchased the eCompli software application from a company called Compli, Inc. We are contacting you because we recently learned about a vulnerability in eCompli that resulted in the accidental exposure to a third party of certain personal information that you provided to us. The third party informed us of the vulnerability after discovering it, and subsequently deleted all copies of personal information that they accessed via the vulnerability. The third party also certified that they did not use or share the personal information for any purpose other than as described in this notice. We have taken appropriate steps to address and remove the vulnerability, and our investigation indicated that this third party was the only party that accessed the personal information via the vulnerability.

WHAT HAPPENED

On May 22, 2019, an employee of one of our customers (who happens to be a former employee of Compli, Inc.) notified us that an eCompli code update contained a vulnerability that allowed the employee to gain unauthorized access to certain personal information about certain individuals at some of our customers, including your organization. This third party informed us of the vulnerability and we subsequently removed the vulnerability on May 22, 2019.

WHAT INFORMATION WAS INVOLVED

The types of personal information that were exposed included users' first and last names, organization, social security number, driver's license number and state, contact information, date and place of birth, citizenship status, eye and hair color, weight, height, marital status, marriage date and place, employment history, residence history and State Alcohol Board license number and date of expiration. The third party that discovered the vulnerability informed us of the vulnerability and subsequently certified to us that they did not share with any other party, and deleted all copies of, the information they accessed via the vulnerability. We have also confirmed by reviewing our internal logs that this third party was the only entity who accessed personal information via the vulnerability.

WHAT WE ARE DOING

In response to the notification from this third party, we promptly conducted an investigation to determine the scope of the incident, confirmed that the vulnerability was removed on May 22, 2019, and took all reasonable and appropriate actions to ensure that the security and integrity of our platform has been restored. We and our service providers have reviewed our security protocols and taken steps to address the security of the platform. We and our service providers are closely monitoring our platform to help protect against future unauthorized access.

WHAT YOU CAN DO

In addition to reviewing the items discussed below, we encourage you to remain vigilant about any suspicious activity involving your personal information.

OTHER IMPORTANT INFORMATION

Please consider the following additional information:

- You may wish to visit the website of the U.S. Federal Trade Commission at http://www.consumer.ftc.gov/features/feature-0014-identity-theft or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.

- You may have the right to obtain any police report filed related to this intrusion, and to file a police report and obtain a copy of it if you are the victim of identity theft.

- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.

- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: *(1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses over the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint*. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

    - Experian: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
    - Equifax: 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348
    - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

- You have relevant rights pursuant to the federal Fair Credit Reporting Act. For more information, please see the U.S. Federal Trade Commission's bulletin on Fair Credit Reporting Act rights available here: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

- We are also offering you a period of credit monitoring services at no cost to you. Please call 805-226-5350 for information on obtaining such services.

FOR MORE INFORMATION

If you have further questions or concerns, please contact us at 805-226-5350.

Sincerely,

Avalara, Inc.