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.
- 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.