RUTAN
RUTAN & TUCKER, LLP

Michael T. Hornak
Direct Dial: (714) 641-3472
E-mail: mhornak@rutan.com

May 24, 2017

VIA ELECTRONIC MAIL

Office of the Washington Attorney General
Attn: Security Breach Notification

SecurityBreach@atg.wa.gov

Re: Data Incident Potentially Affecting Personal Information of Washington Residents

To whom it may concern:

On behalf of our client, Incipio, LLC ("Incipio," or the "Company"), located at 6001 Oak Canyon, Irvine, California 92618, we write to notify you of a data security incident at Aptos, one of the Company's former vendors, that may have compromised the security of personal information of 1,650 Washington residents, 42 of which involved active payment cards.

Nature of the Data Security Event

Aptos was a former digital commerce solution provider for Incipio, and recently advised the Company that Aptos' systems had been compromised, and that unidentified persons had gained access to customer data for forty of Aptos' online retailer customers, including Incipio. Aptos reports that the unauthorized access to its systems occurred from approximately February 26, 2016, through approximately December 5, 2016. Notice to Incipio was delayed because of a law enforcement investigation. Aptos has since reported the incident to various state and regulatory authorities, likely including those in your State.

The information potentially accessed likely included information on Incipio customers, including name, address, phone number, email address, credit or debit card number, and the customer's payment card's expiration date, but not the cvv2 number. The information accessed involved customers who transacted business on myincipio.com from November 2010 to September 2012, on bespoike.incipio.com from December 2010 to October 2015, and on shop.myincipio.com/blackberry from June 2010 to August 2013. The large majority of customers' affected payment cards are reported to have been expired at the time of the unauthorized access. Aptos has advised that it is unaware of any instance of fraud or identity theft arising from the incident.

Aptos has advised its retail online customers, including Incipio, of various steps it has taken to improve security and prevent further incidents, including but not limited to quarantining malicious files, hiring outside professionals, and other remediation activities. Aptos advises that

it has worked with law enforcement to supply them with the numbers of the affected cards to provide to card issuers for monitoring.

Number of Washington Residents Affected

The number of Washington residents potentially affected by this data incident

is 1,650, of which Aptos records reflect that only 42 involved payment cards that were not expired. Notice by mail is being sent promptly, within the next three business days, to all residents potentially affected. A copy of the notice template is attached.

Additional Steps Taken and To Be Taken

The security breach did not happen on Incipio's servers, and Incipio no longer utilizes Aptos as a vendor or service provider. Incipio has instructed Aptos to delete all Incipio customer information from Aptos' servers. Thus, any future security breaches at Aptos should not affect Incipio customers. Incipio is providing notice of the data incident to certain state regulators and law enforcement in accordance with various state notification laws.

Other Notification and Additional Information

We trust that this letter and its attachment provide all the information required to assess this incident and the Company's response. Do not hesitate to contact the undersigned should you have any questions or if we may be of further assistance.

Very truly yours,

RUTAN & TUCKER, LLP

Michael T. Hornak

MTH:ms
Attachment

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

On behalf of Incipio, LLC, I am writing to tell you about a data security incident at a former vendor, Aptos, which may have exposed some of your personal information. We understand the importance of protecting your personal information and are contacting you directly to explain the circumstances of the incident, although we are unaware of any actual misuse of your information.

What happened?

Aptos, our former digital commerce solution provider, recently advised us that its systems had been compromised, and that unidentified persons had gained access to customer data for forty of Aptos' online retailer customers, including Incipio. Aptos reports that the unauthorized access to its systems occurred from approximately February 26, 2016, through approximately December 5, 2016. Notice to us was delayed because of a law enforcement investigation.

What information was involved?

The information accessed likely included your name, address, phone number, email address, payment card number ending in <<ClientDef1(Card Number)>>, and your payment card's expiration date. No cvv2 data is believed to have been compromised. The information accessed involved customers who transacted business on myincipio.com from November 2010 to September 2012, on bespoke.incipio.com from December 2010 to October 2015, and on shop.myincipio.com/blackberry from June 2010 to August 2013. Aptos advises that it is unaware of any instance of fraud or identity theft arising from the incident.

What we are doing.

The security breach did not happen on our servers, and Incipio no longer utilizes Aptos as a vendor or service provider. Incipio has instructed Aptos to delete all Incipio customer data from its systems. Aptos has advised us of various security measures it has taken since the incident, including deleting malicious code, and that it has worked with law enforcement to help supply them with the numbers of the affected cards to card issuers for monitoring.

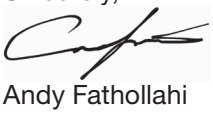
What you can do.

Notwithstanding the efforts taken to protect your personal data, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please email us at datasecurity@incipio.com. Protecting your information is important to us. We deeply regret the events at Aptos leading to this notice. We are committed to your security and satisfaction.

Sincerely,



Andy Fathollahi
Chief Executive Officer
Incipio

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.