aptos

945 East Paces Ferry Rd., Suite 1475, Atlanta, GA 30326
+1-866-493-7037 aptos.com

April 4, 2017

BY U.S. MAIL

Office of Consumer Protection
Department of Commerce and Consumer Affairs
Leiopapa A. Kamehameha Building
235 South Beretania Street, Suite 801
Honolulu, Hawaii 96813

To Whom It May Concern:

Referring to our previous letter dated February 25, 2017, and consistent with Haw. Rev. Stat. Ann, § 487N-2, this letter provides supplemental notice on behalf of an additional Retailer. This Retailer is notifying a total of 1,302 Individual Consumers with billing addresses in Hawaii. Please see the attached schedule and consumer notice for further details.

Aptos is committed to full cooperation in answering any questions that your office may have. Please feel free to contact me with any questions at securityinfo@aptos.com.

Respectfully yours,

/s/

David Baum
Senior Vice President, General Counsel

Enclosures

Retailer Name	Plow and Hearth, LLC
Contact Information	7021 Wolftown-Hood Road Madison, VA 22727 Leslie Newton, COO 540-948-2272 lnewton@plowandhearth.com
Number of Individual Consumers Notified in This Jurisdiction	1,834 [Retailer notes that based upon communications from Aptos, no PIN or SSN data for its customers was exposed]
Date Individual Consumers Notified	Between 2/27/17 and 3/14/17
Form of Individual Consumer Notification	Mail

Plow & Hearth 7021 Wolftown-Hood Rd., Madison, VA 22727
540.948.2272 www.plowandhearth.com

[Insert date]

[Name]
[Address]
[City], [State] [ZIP]

Dear **[Name]**,

We are writing to notify you of an incident that involves certain of your personal information. The third-party company contracted to operate our e-commerce platform, Aptos, Inc. ("Aptos"), which also supports our brands Wind & Weather, HearthSong, Magic Cabin, and Problem Solvers, and formerly supported our subsidiary's brand Reuseit, informed us on February 6, 2017, that it had experienced a malware intrusion of its systems last year. To date, the investigation indicates that the intrusion on Aptos' systems occurred between February 2016 and December 2016, and included access to certain of our customers' personal information for transactions during that time period, as well as transactions dating back to 2013. The personal information involved in the incident may have included your name, address, phone number and payment card information (including expiration dates and, in limited cases, security codes). Our records indicate that your credit card(s) ending in [xxxx] was impacted.

We have been informed that Aptos is working with a leading cybersecurity firm and has taken steps to secure systems and determine the nature of the incident. Aptos is also working with law enforcement authorities in their investigation. The credit card companies and issuing banks are being contacted for the purposes of identifying unauthorized charges.

Based on the information we have at this time, there is no evidence that any of the information has been misused as a result of this incident. We regret that this incident may affect you. We take our obligation to safeguard personal information very seriously and are alerting you about this incident so you can take steps to help protect yourself. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.

We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. Furthermore, the attached Reference Guide provides recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We hope this information is useful to you. If you have any questions regarding this incident, please call **1-800-303-0562, Monday through Friday 9:00am to 6:00pm, eastern standard time.**

Again, we regret any inconvenience this may cause you.

Sincerely,

Dana Pappas, CFO

Reference Guide

We encourage our affected customers to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office as it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends the following steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
http://www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
http://www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

aptos

945 East Paces Ferry Rd., Suite 1475, Atlanta, GA 30326
+1-866-493-7037 aptos.com

February 25, 2017

BY U.S. MAIL

Office of Consumer Protection
Department of Commerce and Consumer Affairs
Leiopapa A. Kamehameha Building
235 South Beretania Street, Suite 801
Honolulu, Hawaii 96813

To Whom It May Concern:

Consistent with Haw. Rev. Stat. Ann, § 487N-2, this letter provides notice of a computer data security incident. Aptos, Inc. ("Aptos") contracts with a number of online retailers ("Retailers") who in turn do business with their Consumers ("Individual Consumers"). Aptos provides a digital commerce platform that functions as the back-end for the Retailers' online stores, as well as an order management system utilized by certain Retailers. As a result, Aptos holds the data of Individual Consumers associated with their transactions at a number of online stores operated by various Retailers.

Aptos has determined that there has been remote access intrusion to its systems that resulted in unauthorized access to information of Individual Consumers. Aptos provides this notice on behalf of those Retailers on the attached schedule. For those Retailers, the intrusion resulted in access to online transaction data including Individual Consumers' first and last names, addresses, phone numbers, payment card numbers, and expiration dates. In certain instances, CVV2s may have been exposed.

Each Retailer has determined the number of Individual Consumers in your state to whom it will send notice. The number of Individual Consumers receiving notice from each Retailer is listed on the attached schedule, along with contact information for each Retailer and information about the Retailer's distribution of notices to Individual Consumers.

Our investigation indicates that the intrusion began in approximately February 2016 and ended in approximately December 2016. The Retailers on the attached schedule are notifying a total of 3,002 Individual Consumers with billing addresses in Hawaii.

Aptos discovered indications of this intrusion in late November 2016, and promptly reported this matter to the FBI and the U.S. Department of Justice. Law enforcement requested that Aptos not notify the Retailers before February 5, 2017. Aptos gave notice to affected Retailers on February 6, and thereafter provided Individual Consumer contact information to affected Retailers. We are unaware of any reports of payment card fraud or other misuse of the data at issue.

In response to these events, Aptos has worked with a leading cybersecurity firm to remove the malware from its systems and to make security updates to the systems, including strengthening access controls.

Aptos is committed to full cooperation in answering any questions that your office may have. Please feel free to contact me with any questions at securityinfo@aptos.com.

Respectfully yours,

/s/

David Baum
Senior Vice President, General Counsel

Enclosures