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 the Attorney General
Director of the Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319

To Whom It May Concern:

Consistent with Iowa Code Ann. § 715C.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 7,441 Individual Consumers with billing addresses in Iowa.

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

Schedule

Retailer Name	Atlantic Cigar
Contact Information	c/o Davis Wright Tremaine LLP 1919 Pennsylvania Ave. NW, Suite 800 Washington, DC 20006 Christin McMeley Davis Wright Tremaine 202-973-4264 christinmcmeley@dwt.com
Number of Individual Consumers Notified in This Jurisdiction	3,063 [Retailer notes that, as to its customers, no PIN or CVV or SSN data was exposed]
Date Individual Consumers Notified	On or about 3/1/2017
Form of Individual Consumer Notification	Mail

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	595 [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	Email

Retailer Name	Theisen's Inc.
Contact Information	6201 Chavenelle Rd. Dubuque, IA 52002 Brannon Dixon, President 563-556-4738 brannond@theisens.com
Number of Individual Consumers Notified in This Jurisdiction	3,783
Date Individual Consumers Notified	TBD
Form of Individual Consumer Notification	Mail

3 Horne Drive Suite 102
Folcroft, PA 19032
844-371-5335
10 a.m. – 5:30 p.m. EST daily

[Date]

«First_name» «Last_name»
«Address_1», «Suite/Apt»
«City», «State» «Zip»

NOTICE OF DATA BREACH

Dear «First_name» «Last_name»,

We are writing to notify you about a security incident that involves your payment card information.

What Happened? We use a third party service provider, Aptos, to maintain our database of customer ordering information. In November 2016, Aptos discovered indications that its systems had been compromised and promptly reported its suspicions to U.S. law enforcement agencies, who requested Aptos delay any notification of the incident to third parties, including Atlantic Cigar Co., during the criminal investigation. On February 10, 2017, Aptos notified us that there had been remote access intrusion to Aptos' systems that resulted in unauthorized access to our customers' information. At this time, we are unaware of any reports of credit card fraud or other misuse of our customers' data.

What Information Was Involved? The intrusion resulted in access to online transaction data, including your first and last name, billing and shipping address(es), phone number, payment card information including account number and expiration date.

What We Are Doing. In response to these events, Aptos has worked with a leading cybersecurity firm to remove the malware from and update the security of its systems, including strengthening access controls. Additionally, Atlantic Cigar Co. has arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 13 months:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID_Phone» and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: {Redemption_Code}.

Additional steps may be required by you in order to activate your phone alerts and monitoring options.

Other Important Information. Please review the "Further Steps and Contact List" information on the reverse side of this letter which identifies additional steps to take to protect your information.

For More Information. If you have further questions or concerns about this incident, please call AllClear ID, Monday through Saturday, 8 a.m. – 8 p.m. CST.

We take all privacy and security incidents seriously. We deeply regret any inconvenience this may cause you, and thank you for your understanding.

Sincerely,

Paul Scipioni
President

(see reverse side)

FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION
CONTACT LIST

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	annualcreditreport.com

Fraud Alert

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

We will **NOT** send you any electronic communications regarding this incident and ask you to disclose any personal information.

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.

THEISEN'S LETTERHEAD

[DATE]

Name
Address
City State Zip

RE: Notice of Data Breach

Dear [Recipient Name]:

Theisen's Inc., ("Theisen's"), is writing regarding a recent data security incident that may impact the demographic and payment card information you used on our e-commerce website. We wanted to provide you with information about this incident, our response, and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? On February 8, 2017, we received information from Aptos, the company that hosts and manages our e-commerce site, that customer information stored in their system had been compromised by malicious software injected into the Aptos system sometime in February, 2016. This malicious software allowed the attacker to capture sensitive customer information prior to encryption as well as decrypt historical credit card information stored on the site. Upon learning of this incident, we immediately began an investigation to identify what happened and what information may be impacted. Aptos has been working with the FBI and the U.S. Department of Justice since they discovered the intrusion and have only recently received permission from the FBI to notify us about this incident.

What Information Was Involved? Aptos is reporting that customer demographic and credit/debit card information entered on our e-commerce site between February 2016 and December 2016 was accessed by an unknown actor. In addition to payment information entered between February and December, 2016, the intruder also had access to historical payment card information stored by Aptos. The information accessed includes the cardholder's name, address, telephone number, email address, card number, card type and expiration date. While the card number and other card data was encrypted, Aptos reports that the bad actor was able to decrypt the card data.

What We Are Doing. We take this incident, and information security, very seriously at Theisen's. We are diligently investigating this incident, and we are currently taking steps to obtain additional information from Aptos. We are also working to ensure that Aptos is taking all steps necessary to protect our customer information. Additionally, we are providing written notice of this incident to those who may be impacted so that they can take steps to prevent possible fraud. Certain state regulators are also being notified about this incident.

What You Can Do. You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud", which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

As an added precaution, we have arranged to have Experian to provide you with CSID Protector services, including CyberAgent® Internet Surveillance and Identity Theft Insurance, for 12 months at no cost to you. The following identity protection services start on the date of this notice, and you can use them at any time during the next 12 months. The cost of this service will be paid for by Theisen's. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in identity monitoring.

CSID Protector includes:

- CyberAgent®: CSID's Internet surveillance technology scours websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- Identity Theft Insurance: You are eligible for reimbursement for certain expenses in the event that your identity is compromised with a $1,000,000 insurance policy that has been issued to CSID.
- Identity Restoration: Work with a certified identity theft restoration specialist, who will work on your behalf to restore your identity and let you get on with your life

You can sign up for these services by doing the following:

- Visit https://www.csid.com/csid1yprotector/ to complete a **secure** sign up process and answer some questions to confirm your identity.
- Submit your PIN Code: [PIN code] This PIN Code can only be used once and cannot be transferred to another individual.
- Activate your CSID Protector coverage by no later than [Enrollment End Date].

Additionally, Identity Restoration services are available to you as of [DATE], with no further action required. If you are a victim of fraud, simply call CSID at (877) 926-1113 by no later than [Enrollment End Date] and a dedicated Identity Theft Restoration agent will help you restore your identity. Please provide the PIN Code in this letter as proof of eligibility.

For More Information. We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at XXXX, XX through XX, XX a.m. to XX p.m. E.S.T (excluding U.S. holidays).

Sincerely,

[Signature]

NAME/TITLE

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also 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. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also 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. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com
https://www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service

Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. **For Rhode Island residents**, Attorney General can be contacted at (401) 274-4400, http://www.riag.ri.gov, or 150 South Main Street, Providence, RI 02903. Approximately XX Rhode Island residents may be impacted by this incident. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement.

Aptos, Inc.
945 East Paces Ferry Road
Suite 2500
Atlanta, GA 30326

PLACE STICKER AT TOP OF ENVELOPE TO THE RIGHT OF THE RETURN ADDRESS. FOLD AT DOTTED LINE.

CERTIFIED MAIL

7016 0910 0000 4731 7473

Office of the Attorney General of Iowa
Director of the Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319