

October 10, 2017

Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notice

To Whom It May Concern:

I represent Atlantic Cigar Company, LLC ("Atlantic"). This letter is being sent because Atlantic learned via letter from its payment card processing and database provider, Aptos, that an unauthorized third party accessed payment card information of 9 residents, which was stored on Aptos' systems.

In its letter, dated August 25, 2017, and subsequent FAQ document, Aptos reported that the security incident lasted from July 21, 2017 to August 9, 2017. Aptos further represented that it engaged a cybersecurity firm to remediate the incident, and that it has been in contact with the FBI. Atlantic has integrated Aptos' payment card processing software into its e-commerce website, which tokenizes any such information. Atlantic does not receive or store any payment card data on its systems. Atlantic received a list of potentially affected customers from Aptos on September 11, 2017, and immediately began the process of making customer and regulatory notifications.

Atlantic will begin notifying its customers on October 11, 2017 using the attached letter. As referenced in the letter, Atlantic will provide 12 months of credit monitoring and identity protection services to affected consumers through AllClear ID. Please contact me should you have any questions.

Sincerely,

Davis Wright Tremaine LLP



Amy Mushahwar

cc: Paul Scipioni, President



Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

October 11, 2017

NOTICE OF DATA BREACH

Dear John Sample,

We are writing to notify you about a security incident that reportedly resulted in the unauthorized acquisition of your payment card information.

What Happened? We use a third party service provider, Aptos, to maintain our database of customer ordering information. Aptos notified us on August 25, 2017 that unauthorized third parties gained access to its systems, and that this security incident lasted from July 21, 2017 to August 9, 2017.

What Information Was Involved? The intrusion resulted in access to the following information: name, postal address, email address, and payment card data including credit card number, expiration date, and card verification numbers.

What We Are Doing. Aptos worked with a leading cybersecurity firm to prevent further intrusions into its systems. We are in the process of updating our website to make our payment systems more secure.

We have 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 12 months:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-904-5757 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 or by phone by calling 1-855-904-5757 using the following redemption code: Redemption Code.

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

Other Important Information. Please review the information on the reverse side of this letter which identifies additional steps you may take to protect your information.

For More Information. For further information and assistance, please contact us at 1-855-904-5757 from Monday - Saturday, 8am - 8pm CT, excluding National Holidays.

We care deeply about the privacy and security of your personal information. We regret any inconvenience this may cause you, and thank you for your understanding.

Sincerely,

Paul Scipioni
President



01-01-1-00

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 (from whom you may be able to obtain a police report), 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/manualRequestForm.action>. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
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 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

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland

Attorney General
200 5t. Paul Place
Baltimore, MD 21202
www.oag.state.md.us
1-888-743-0023

North Carolina

Attorney General
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
1-877-566-7226

Rhode Island

Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

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

Massachusetts residents have the right to obtain a police report.