Baker McKenzie.

Baker & McKenzie LLP

Two Embarcadero Center, 11th Floor
San Francisco, CA 94111-3802
United States

Tel: +1 415 576 3000
Fax: +1 415 576 3099
www.bakermckenzie.com

Asia Pacific
Bangkok
Beijing
Brisbane
Hanoi
Ho Chi Minh City
Hong Kong
Jakarta
Kuala Lumpur*
Manila*
Melbourne
Seoul
Shanghai
Singapore
Sydney
Taipei
Tokyo
Yangon

Europe, Middle East & Africa
Abu Dhabi
Almaty
Amsterdam
Antwerp
Bahrain
Barcelona
Berlin
Brussels
Budapest
Cairo
Casablanca
Doha
Dubai
Dusseldorf
Frankfurt/Main
Geneva
Istanbul
Jeddah*
Johannesburg
Kyiv
London
Luxembourg
Madrid
Milan
Moscow
Munich
Paris
Prague
Riyadh*
Rome
St. Petersburg
Stockholm
Vienna
Warsaw
Zurich

The Americas
Bogota
Brasilia**
Buenos Aires
Caracas
Chicago
Dallas
Guadalajara
Houston
Juarez
Lima
Los Angeles
Mexico City
Miami
Monterrey
New York
Palo Alto
Porto Alegre**
Rio de Janeiro**
San Francisco
Santiago
Sao Paulo**
Tijuana
Toronto
Valencia
Washington, DC

* Associated Firm
** In cooperation with Trench, Rossi e Watanabe Advogados

CONFIDENTIAL

July 05, 2019

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street, Concord, NH 0330

By certified mail
Recipient's Delivery Details

Notice of Data Breach

Dear Mr. MacDonald,

I write on behalf of Inter-Continental Cigar Corporation ("**ICC**") to notify you that ICC recently learned that its online store at www.on-nicotine.com (the "**Site**"), which is managed by a third party website technology services provider, was exposed to a security breach that potentially resulted in the unauthorized acquisition of certain personal information that ICC customers submitted.

On June 19, 2019, ICC received a report about a potential compromise to a credit card used by one of its customers. ICC expediently reached out to the third-party website technology services provider who designed, built, and maintains the Site as part of a managed services arrangement to gather information about the suspected incident, and also engaged an external forensic investigator who examined the Site. On June 28, 2019, ICC's investigation determined that malicious code had been added to the Site code which caused the names, addresses, credit card numbers, credit card expiration dates and credit card security codes (CVVs) that customers submitted in connection with making a purchase on the Site to be potentially exposed to unauthorized persons, possibly for purposes of committing credit card fraud.

ICC's IT specialists determined that the Site is the only ICC website to include this vulnerability. ICC instructed its website services provider to take the Site offline and received confirmation that this was completed at 7:18 a.m. (Eastern Time) on June 28, 2019. ICC's IT specialists have confirmed that the vulnerability cannot be exploited while the Site is offline, so there is no continued threat. The Site was launched on October 18, 2018, and ICC is investigating when the malicious code was injected to the Site code.

ICC plans to work with payment card providers to prevent any harm or hassle to affected customers. ICC has engaged information security specialists who are reviewing and improving on the Site's security measures, and ICC will conduct third-party vulnerability testing before it re-launches the Site to protect against this and other forms of malicious code. ICC and its service providers will closely monitor all of ICC's websites to help protect against future unauthorized access.

Baker McKenzie.

ICC is offering credit monitoring services to affected data subjects free of charge. ICC is providing on July 5, 2019 postal mail notifications to impacted individuals informing them of the incident, and encouraging them to take security precautions regarding their personal information. The number of affected data subjects in New Hampshire is 3.

Affected individuals may contact ICC at 1-866-775-4209. We attach a copy of ICC's sample data subject notice. Please feel free to contact me directly at 415-984-3883 or jonathan.tam@bakermckenzie.com.

Best regards,

Jonathan Tam.

Jonathan Tam

Attorney

Inter-Continental Cigar Corporation
3251 Commerce Parkway
Miramar, FL 33025

July 5, 2019

[*Name of Data Subject*]
[*Address*]

NOTICE OF DATA BREACH

Thank you for being a customer of Inter-Continental Cigar Corporation (ICC). We are contacting you because we recently learned that our online store at www.on-nicotine.com (the "**Site**"), which is managed by a third party website technology services provider, was exposed to a security breach that potentially resulted in the unauthorized acquisition of certain personal information that ICC customers submitted.

WHAT HAPPENED

On June 19, 2019, we received a report about a potential compromise to a credit card used by one of our customers. We expediently reached out to the third-party website technology services provider who designed, built, and maintains the Site as part of a managed services arrangement to gather information about the suspected incident, and also engaged an external forensic investigator who examined the Site. On June 28, 2019, our investigation determined that malicious code had been added to the Site code which caused certain personal information that customers submitted in connection with making a purchase on the Site to be potentially exposed to unauthorized persons, possibly for purposes of committing credit card fraud.

Our IT specialists determined that the Site is the only ICC website to include this vulnerability. We instructed our website technology services provider to take the Site offline and received confirmation that this was completed at 7:18 a.m. (Eastern Time) on June 28, 2019. Our IT specialists have confirmed that the vulnerability cannot be exploited while the Site is offline, so there is no continued threat. The Site was launched on October 18, 2018, and we are investigating when the malicious code was injected to the Site code.

WHAT INFORMATION WAS INVOLVED

The types of personal information that may have been exposed include customers' first and last names, addresses, credit card numbers, credit card expiration dates, and credit card security codes (CVVs).

WHAT WE ARE DOING

We have taken the Site offline and notified all potentially affected customers. We are working with payment card providers to prevent any harm or hassle to affected customers. We have engaged information security specialists who are reviewing and improving on the Site's security measures, and we will conduct third-party vulnerability testing before we re-launch

the Site to protect against this and other forms of malicious code. We and our service providers will closely monitor all of our websites 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.

- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.

- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can 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. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may 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. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: *(1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses over the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint*. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

- Experian: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
- Equifax: 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348
- TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

- You have relevant rights pursuant to the federal Fair Credit Reporting Act. For more information, please see the U.S. Federal Trade Commission's bulletin on Fair Credit Reporting Act rights available here: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

- To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. To receive these services online or by mail, please call 1-866-775-4209. You will then be sent details by mail as to how to activate your identity monitoring services. You have until October 11, 2019 to request and activate the monitoring services.

FOR MORE INFORMATION

If you have further questions or concerns, please contact us at 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Inter-Continental Cigar Corporation