Cooley

Andrew B. Epstein
+1 720 566 4203
aepstein@cooley.com

VIA EMAIL TO: ndag@nd.gov

August 8, 2019

Office of Attorney General
North Dakota
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040

**Re: Legal Notice of a Potential Information Security Incident**

To Whom It May Concern:

On behalf of our client, Cable One, Inc. ("Cable One"), I write to provide you with notice of a potential data incident that may affect approximately six hundred fifty four (654) North Dakota residents. Although Cable One did not confirm that any personal information was accessed or acquired as a result of this potential incident, the company is notifying individuals out of an abundance of caution and providing them with information and steps that they can take to help protect themselves.

Cable One recently learned that an unauthorized individual, through a third-party vendor, obtained access to a limited number of Cable One email accounts. The company promptly engaged an independent information security forensic firm to assist with an investigation of this matter. Cable One believes that some of the affected email accounts may have contained certain information about a limited number of employees and in some cases their beneficiaries, dependents, and others. Potentially affected information varies by individual, but may include information such as first and last name, Social Security number, date of birth, and medical history. Cable One retained an e-discovery and data review firm to help with this determination and to identify details necessary for disclosure to residents. At this time, Cable One has no evidence indicating that any potentially affected information has been or will be misused as a result of this incident.

Cable One takes the privacy of personal information seriously and deeply regrets that this incident occurred. Upon learning of a potential incident, Cable One promptly disabled the third party vendor's access to the company's email systems, reset account passwords and contacted law enforcement. In addition, to help prevent this type of incident from reoccurring in the future, Cable One is continuing to review its security measures and enhance the security of its email system.

Potentially affected residents are being notified via written letter, which will begin mailing on or about August 8, 2019. For residents whose Social Security number may have been affected, Cable One is also offering one year of complimentary credit monitoring services at no charge to the individual. A copy of the template notice being sent to potentially affected residents is enclosed for your reference.

Cable One's investigation of this matter remains ongoing at this time, and we will provide further updates to your office if needed. Should you require any additional information, please do not hesitate to contact me at 720-566-4203 or aepstein@cooley.com.

Sincerely,

Andrew B. Epstein

ABE:ABE

Enclosure

209363640 v1

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

## NOTICE OF DATA INCIDENT

We are writing to inform you of a potential security incident involving certain personal information you provided to Cable One, Inc. ("Cable One"). We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

### *What Happened*

We recently learned that an unauthorized individual, through a third-party vendor, obtained access to a limited number of Cable One employees' email accounts. These employee email accounts contained certain personal information about some of our employees and their dependents and beneficiaries. Our investigation has not found any evidence that this incident involves any unauthorized access to or use of any of Cable One's internal computer systems or network. In addition, we can confirm that **your Cable One email account was not accessed as part of this incident**.

### *What Information Was Involved*

The information stored in the accessed email account varies by individual but may include <<PII Categories>>. Based on our investigation, it appears you are one of the individuals whose information was stored in an accessed account and therefore your information could be affected by this incident. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

### *What We Are Doing*

We take the privacy of personal information seriously and deeply regret that this incident occurred. We took steps to address this incident promptly after it was discovered, including initiating an internal investigation into this incident and retaining an independent forensic investigation firm to assist us in our investigation of and response to this incident. We have also notified federal law enforcement and will continue to cooperate in any investigation. To help prevent this type of incident from reoccurring in the future, we are continuing to review and enhance security measures and access controls for our email system moving forward.

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **November 30, 2019** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your activation code: **<<Activation Code>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by **November 30, 2019.** Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the identity restoration services by Experian.

***What You Can Do***

Although we are not aware of any misuse of your information arising as a result of this incident, we want to make you aware of steps that you can take as a precaution:

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering identity theft protection services at no cost to you. For more information about these services, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter.
- **Checking Credit Reports and Financial Accounts.** You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.
- **Reviewing credit and debit card account statements.** If your credit or debit card numbers may have been affected, you may also wish to review credit and debit card account statements as soon as possible to determine if there are any discrepancies or unusual activity listed. We urge individuals to remain vigilant and continue to monitor statements for unusual activity going forward. If you see something you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should immediately notify the issuer of the credit or debit card. In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.
- **Reviewing Explanation of Benefits Documents.** You can also review explanation of benefits statements that you receive from your health insurer or health plan or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits that were not received, please immediately contact your insurer or health plan.
- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

***For More Information***

For more information about this incident, or if you have additional questions or concerns, you may contact us at 855-821-6808 between the hours of 6 am to 6 pm Pacific time, Monday through Friday. Again, we sincerely regret any concern this incident may cause.

Sincerely,

Julia Laulis
Chief Executive Officer

## INFORMATION ABOUT IDENTITY THEFT PROTECTION

**Additional Details Regarding Your Experian IdentityWorks Membership:** A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

**Review Accounts and Credit Reports:** You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

**For residents of Maryland**: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

**For residents of North Carolina**: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

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

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

**Security Freezes and Fraud Alerts:** You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

**Additional Information for New Mexico Residents:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity;

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and

(4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf, https://www.consumerfinance.gov/learnmore/. or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

**National Credit Reporting Agencies' Contact Information**

Equifax (www.equifax.com)

**General Contact:**
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

**Fraud Alerts and Security Freezes:**
P.O. Box 740256, Atlanta, GA 30374

Experian (www.experian.com)

**General Contact:**
P.O. Box 2002, Allen, TX 75013
888-397-3742

**Fraud Alerts and Security Freezes:**
P.O. Box 9556, Allen, TX 75013

TransUnion (www.transunion.com)

**General Contact, Fraud Alerts and Security Freezes:**
P.O. Box 2000
Chester, PA 19022
888-909-8872