

**BakerHostetler**

**RECEIVED**

**JUN 27 2019**

**CONSUMER PROTECTION**

**Baker & Hostetler LLP**

1170 Peachtree Street  
Suite 2400  
Atlanta, GA 30309-7676

T 404.459.0050  
F 404.459.5734  
www.bakerlaw.com

John P. Hutchins  
direct dial: 404.946.9812  
jhutchins@bakerlaw.com

June 26, 2019

**VIA OVERNIGHT MAIL**

Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, New Hampshire 03301

*Re: Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, Calista Corporation (“Calista”), to notify you of a security incident. Calista Corporation is a regional Alaska Native Corporation, established under the Alaska Native Claims Settlement Act as a means of creating economic opportunities for Alaska Native Shareholders in Southwest Alaska.

Calista recently concluded an investigation and analysis of a phishing attack targeted at Calista, in which a cybercriminal tricked a Calista employee into providing their email account credentials. Upon learning of the attack, the employee’s email account was secured, and a leading forensic investigation firm was engaged to work with us to conduct an investigation. Through its investigation, Calista determined that one or more unauthorized persons accessed the employee’s email account on December 9, 2018. As part of its investigation, Calista undertook a comprehensive review of the emails and attachments in the employee’s email account. Although Calista was able to determine the name and address of some of the affected individuals on April 19, 2019, many of the source files did not include the addresses of the affected individuals. Calista continued to investigate the addresses of additional affected individuals and determined on May 29, 2019 that the name, address, and Social Security number of two New Hampshire residents may have been involved.

Calista began mailing notification letters on June 20, 2019 via United States Postal Service First-Class mail to two New Hampshire residents, in accordance with N.H. Rev. Stat. Ann. § 359-

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

June 26, 2019

Page 2

C:20c.<sup>1</sup> A copy of the notification letter is enclosed. Calista will be offering all individuals whose Social Security numbers and/or driver's license numbers may have been involved complimentary one-year memberships to a credit monitoring and identity theft protection service through Experian®. Calista is providing notice as soon as possible and without unreasonable delay after completing its investigation of the incident and determining the addresses of the individuals involved.

To help prevent something like this from happening in the future, Calista is providing additional training to their employees regarding phishing emails and other cybersecurity issues. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in blue ink that reads "John P. Hutchins". The signature is written in a cursive style.

John P. Hutchins  
Partner

Enclosure

---

<sup>1</sup> This report is not, and does not constitute, a waiver of Calista's objection that New Hampshire lacks personal jurisdiction over this matter.



CALISTA CORPORATION

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Calista Corporation ("Calista") is committed to protecting the personal information of its shareholders and other individuals affiliated with Calista. We are writing to inform you that we recently identified and addressed a security incident that may have involved your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

We recently completed an investigation and analysis of a phishing attack targeted at Calista, in which a cybercriminal tricked a Calista employee leading to the email account credentials being compromised. Upon learning of the attack, the employee's email account was immediately secured, and a leading forensic investigation firm was engaged to work with us to conduct an investigation. Through its investigation, Calista determined that one or more unauthorized persons accessed the employee's email account on December 9, 2018, and as a result may have accessed emails and attachments in the account. In order to determine whether any personal information regarding others may have been accessed, Calista undertook a comprehensive review of the emails and attachments in the employee's email account. Through this review, on April 4, 2019 Calista determined that emails and attachments in the employee's account may have contained your name and some of the following information: Social Security number, driver's license number, U.S. passport number, retirement account information, payment card information, or bank account information.

We wanted to let you know this happened. As a precaution, we have secured the services of Experian® to offer you a complimentary one-year membership of Experian's IdentityWorks<sup>SM</sup>. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter.** Identity Restoration assistance is immediately available to you.

We regret any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we are providing additional training to our employees regarding phishing emails and other cybersecurity issues. In addition, we are enhancing existing security measures related to our email system.

If you have any questions, please call 1-800-277-0015, Monday through Friday from 8:00 a.m. to 5:30 p.m. Pacific Time.

Sincerely,

*Noelle Kompkoff*

Noelle Kompkoff  
Associate Counsel

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<ClientDef1(Enrollment Date)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks** website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Member ID>>

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 877-288-8057. Be prepared to provide engagement number <<ClientDef2(Engagement Code)>> as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## **Additional Steps You Can Take**

Regardless of whether you choose to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity.

You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

### **Equifax**

P.O. Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
(800) 685-1111

### **Experian**

P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
(888) 397-3742

### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
(800) 680-7289

If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

### **Federal Trade Commission**

600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

**If are you a resident of West Virginia**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)

**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)



In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.