LEWIS BRISBOIS BISGAARD & SMITH LLP

Todd Rowe
550 West Adams Street
Suite 3001
Chicago, IL 60661
Todd.Rowe@lewisbrisbois.com
Direct: 312.345.1718

September 26, 2022

VIA EMAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110

Re: *Notification of Data Security Incident*

Dear Attorney General Formella:

Lewis Brisbois Bisgaard & Smith LLP represents Oregon Public Broadcasting (OPB), in connection with a recent data security incident that may have affected the information of certain New Hampshire residents. The purpose of this letter is to notify you of the incident in accordance with New Hampshire data breach notification statute.

1. Nature of the Security Incident

OPB observed unusual activity involving an OPB email account on May 4, 2022 that allowed unauthorized access to the account. OPB immediately suspended access to the account and launched an investigation with the assistance of a leading independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. Through its forensic investigation, OPB concluded that the email account had been accessed without authorization on May 4, 2022.

OPB also engaged independent experts to conduct a review of data that could have potentially been accessed as a result of the incident, and, on September 2, 2022, determined that the information related to its client's employees and members, including the personal information of one New Hampshire resident. To date, OPB has no knowledge that any of this information has been misused.

2. Number of New Hampshire Residents Involved

OPB started notifying one resident of this data security incident via first class U.S. mail on September 26, 2022. A sample copy of the notification letter sent to the affected individuals is attached. The information involved differ depending on the individual but may include name, address, date of birth, Social Security Number and passport number.

The letter sent to the affected individuals notifying them of the incident offers complimentary identity monitoring services and provides additional steps they can take to protect their personal information.

3. Steps Taken Relating to the Incident

In response to the incident, OPB retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise and to prevent similar incidents from occurring in the future. In addition, OPB is in the process of reviewing its current security protocols and adding additional security measures.

As discussed above, OPB is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

OPB is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Todd Rowe at Todd.Rowe@lewisbrisbois.com or (312) 345-1718.

Sincerely,

Todd Rowe of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl.: Sample Individual Notification Letter

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

<<Mail ID>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data <<Variable Header>>

Dear <<Name 1>>,

We are writing to inform you of a data security incident that may have affected some personal information you provided to Oregon Public Broadcasting (OPB). We take the privacy and security of personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary identity protection services we are making available to you.

What Happened: On May 4, 2022, OPB observed unusual activity involving an OPB email account. Upon discovering this activity, we immediately suspended access to the account and launched an investigation with the assistance of a leading independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation concluded that an OPB email account had been accessed without authorization on May 4, 2022. The forensic firm then launched a comprehensive review of the contents of the email account. On September 2, 2022, we learned that some of your information was contained within the account and that you should be notified.

The forensic investigation has not found evidence of any personal information exfiltrated and we have no reason to believe that your information has been misused as a result of this incident at this time.

Since that time, we have been gathering current mailing addresses so that we could notify all potentially affected individuals.

What Information Was Involved: The information may have included your name and address, <<data elements>>.

What We Are Doing: As soon as we discovered this incident, we took immediate investigative action. We have followed all recommendations of the forensics firm and also implemented additional safeguards to help ensure the security of our email environment and to reduce the risk of a similar incident occurring in the future.

To help relieve concerns and to help protect your identity following this incident, we are providing you with information about steps you can take to help protect your personal information, and offering you identity monitoring and protection services through Equifax, a data security and recovery services expert. Your complimentary Equifax identity monitoring and protection services include: 24 months credit monitoring, up to $1,000,000 of identity theft insurance coverage, identity restoration, WebScan notifications, automatic fraud alerts and daily access to your Equifax credit report. Additional information about these services is included with this letter. To take advantage of these services, you must follow the instructions in this letter to enroll. Services will begin upon registration.

What You Can Do: Please read the recommendations included with this letter which you can follow to help protect your personal information. **You can also enroll in the complimentary services being offered to you, at no cost**. Activation instructions and a description of the services being provided are included with this letter.

For More Information: If you have questions or need assistance, please contact 1-888-672-0614, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time, excluding major U.S. holidays. Representatives can help answer questions you may have regarding the protection of your information. We take your trust in us and this matter very seriously. The protection of your personal information remains our top priority, and we've been working diligently to ensure that this type of incident does not happen again. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Steven M. Bass, president & CEO
Oregon Public Broadcasting
7140 S. Macadam Avenue
Portland, OR 97219
<<OPB Phone Number>>

Steps You Can Take to Protect Your Personal Information

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 2000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alert: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Security Freeze: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

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

California: California Attorney General can be reached at: P.O. Box 944255, Sacramento, CA 94244-2550; 1-800-952-5225; https://oag.ca.gov/consumers

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, https://ag.ny.gov/.

Oregon: Oregon Attorney General can be reached at: 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; AttorneyGeneral@doj.state.or.us

Washington: Washington Attorney General can be reached at: 1125 Washington Street SE, PO Box 40100, Olympia, WA 98504-0100; 1-360-753-6200; https://fortress.wa.gov/atg/formhandler/ago/ContactForm.aspx

Enter your Activation Code: ***<<ACTIVATION CODE>>***
Enrollment Deadline: ***<<Enrollment Deadline>>***

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** then click "Submit" and follow these 4 steps:

1. **Register**:
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account**:
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity**:
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. *[2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* *[3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com* *[4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*