July 25, 2022

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

VIA EMAIL

SecurityBreach@atg.wa.gov

Subject: Notice of Data Security Incident

Dear Attorney General Ferguson,

Boeing Employees' Credit Union ("BECU") is a Washington state-chartered credit union headquartered in Tukwila, Washington. We are writing to notify your office of a security incident involving personal information related to 311,448 Washington residents.

Nature of Event

On June 6, 2022, BECU became aware of a network security incident impacting the company's print mailing vendor. The vendor notified legal authorities and immediately launched an investigation into this incident. During the course of the investigation, certain BECU files were identified that may have been accessed by an unauthorized third party. On July 5, 2022, BECU identified the consumers and personal information impacted by this incident.

The information subject to unauthorized access includes names, addresses, full account numbers, credit scores, and Social Security numbers of BECU account holders.

Notice to Consumers

On July 25, 2022, BECU began providing written notice of this incident to affected individuals that included an offer of credit monitoring and identity theft protection. A template letter is attached as Exhibit A.

Other Steps Taken

BECU worked with the vendor and a forensics firm to identify how the event transpired and to ensure a secure environment before resuming services with this vendor. BECU has also hired a vendor to manage consumer inquires about this event. Additionally, BECU has notified the three major Credit Reporting Agencies.

Should you have any questions regarding this notification or other aspects of the data security event, please contact Mark Thomson at privacy@becu.org.

Mark Thomson
Chief Compliance Officer, Vice President of Compliance

Enclosures: Consumer Notification Letter

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>>

Important Privacy Protection Notification. Please read this entire letter.

Dear <<Name 1>>:

At BECU, we value your business and respect the privacy of your information, which is why we are writing to let you know about a vendor network security incident that involves your personal information. We encourage you to read this entire letter because it contains important information concerning the security of your account(s) at BECU. It also includes our offer to provide you with one year of credit monitoring protection at no cost to you unless otherwise required by local law. We take the protection of your information very seriously and are contacting you directly to explain the circumstances of the incident. To learn more, visit **becu.org/vendor-incident**.

What happened?
On June 6, 2022, BECU was informed that its printing vendor had experienced a network security incident. At that time, BECU took immediate measures to protect member information by suspending services with the vendor. After the incident occurred, the vendor indicated that some BECU member information in process at the time of the incident was potentially involved. On July 5, 2022, we were able to determine that your personal information was involved after an independent forensics firm had analyzed the compromised data. We sincerely apologize for any inconvenience or concern this incident may cause.

What information was involved?
The information involved may have included your name, address, account number(s), credit score, and Social Security number.

What we are doing.
The security of accounts and the protection of personal information – for you and all our members – are top priorities at BECU. We are committed to ensuring the security of your personal information. BECU worked with the vendor and a forensics firm before resuming services to improve the security of the vendor's environment as well as its effectiveness at preventing and detecting future cybersecurity incidents.

We understand you may have concerns, so we have secured Equifax Credit Watch™ Gold to provide you credit monitoring protection at no cost for one (1) year unless otherwise required by local law.

To take advantage of this offer, go to **www.equifax.com/activate**. Enter your unique Activation Code: <<ACTIVATION CODE>>, then click **Submit** and follow these steps:

1. **Register:** Complete the form with your contact information and click **Continue**.
   Note: If you already have a myEquifax account, click **Sign in here** under the Let's get started header. Once you have successfully signed in, 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. The confirmation page shows your completed enrollment. Click **View My Product** to access the product features.
5. **Enrollment Deadline:** <<Enrollment Deadline>>

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, you can contact our member support line at 877-390-2571 to request an Equifax Minor Monitoring product.

What you can do.
We sincerely apologize for any inconvenience or concern this incident may cause. We recommend that you regularly review your account activity 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 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 below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and 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 identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that 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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 888-766-0008, www.equifax.com
Experian: 888-397-3742, www.experian.com
TransUnion: 800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent.

If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Because the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies, as specified below, to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

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

Federal Trade Commission and State Attorneys General Offices
If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft, including the use of fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Residents of Massachusetts, Maryland, North Carolina, New York, Connecticut, and the District of Columbia can obtain more information about preventing and avoiding identity theft from their Attorneys General using the contact information below.

For Massachusetts residents: You are advised to report any suspected identity theft to law enforcement and that you have the right to obtain a police report.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: You may contact the New York Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1¬800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 202-727-3400, https://oag.dc.gov/about-oag/contact-us.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission, and the Oregon Attorney General.

Questions?
BECU has partnered with Epiq Corporate Services, Inc., to provide member support for this incident. If you have any questions or would like more information about this incident, you can call 877-390-2571, Monday through Friday from 7 a.m. to 7 p.m. Pacific Time.

We take the privacy and security of your information very seriously. We sincerely regret any worry or inconvenience this matter may cause you.

Sincerely,

Ryan Ko
BECU Privacy Compliance Officer