May 26, 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

To whom it may concern,

Please find below details regarding an ATM skimming event that took place in Renton, WA in late March. A deep skimmer was placed at an ATM in Renton, WA at various times between March 26, 2022 and April 2, 2022. BECU became aware of a pattern of fraud in late April and traced the transactions back to cards used at this ATM on April 30, 2022.

At this time, we believe 720 BECU members used their cards at the ATM during the time the skimmer may have been in place. 717 potentially impacted BECU members are Washington state residents. The personal information at issue may include the name, card number, CVV code, magnetic stripe, PIN, and card expiration date. Currently, we have no indication that Social Security numbers, driver's license numbers or other government-issued ID numbers, dates of birth, addresses, phone numbers, other sensitive personal information or online account credentials have been compromised by this incident. For this reason, we believe this event presents a low risk of identity theft.

- When BECU first learned of potential skimming events, we used our existing fraud detection technology to help identify and decline potentially fraudulent transactions. The amount of fraudulent transactions identified and refunded totaled approximately $75,680.
- BECU has turned off all potentially impacted cards and reached out to those members so they may obtain new cards and PINs.
- For those members who reported unauthorized transactions, BECU has reversed those transactions, credited the amount(s) to the affected account and issued a new card. We will continue to support our members in this way if fraudulent activity is discovered.
- We provided members who used the affected ATM during the timeframe listed above with written notice in compliance with applicable state laws (attached is the form of notice provided to members who are Washington state residents).
- For non-members, BECU notified the applicable payment brands of this incident so they may take steps to protect their cardholders.
- BECU ATMs are already equipped with skimming protection that has successfully detected the insertion of typical skimming devices. And we routinely take steps—and devote significant resources—to increase the security of our ATMs to keep up with industry standards and evolving threats. We will learn from this incident and use the information uncovered during our investigation to further bolster our ATM security.

- We have notified and are cooperating with law enforcement regarding this incident.

Please let me know if you have any further questions.

Sincerely,

Ryan Ko
Compliance Privacy Officer

May 16, 2022

<FullName>
<AddressLine1>
<AddressLine2>
<CityName>, <StateCode> <ZipCode5>

Notice of data security incident. Please read this entire letter.

Dear <FullName>,

We are writing to notify you about a data security incident that may have affected your BECU card(s) and the account associated with the card(s).

This letter contains important information about your account security, including steps you should take immediately to ensure the security of your account. The privacy and security of your information is important to us, and we apologize for the concern and inconvenience this incident may cause you.

What happened?
In late April 2022, several members reported fraudulent transactions involving their BECU accounts. We promptly began investigating these reports and found that all of the affected accounts had been accessed recently by members at a specific BECU ATM.

Based on our continued investigation, we believe that a skimming device was unlawfully installed on one BECU ATM location in Renton, Washington for a period of time between March 26 and April 2. **Our records indicate that you used this ATM when a skimming device may have been in use.**

Skimming devices consist of a card reader disguised to look like legitimate ATM equipment, and often include a tiny camera capable of recording PIN entries. The devices can extract data that can then be used for fraudulent transactions. The information taken by skimming devices varies, but may include your name, card number, CVV code, PIN and card expiration date.

What information was involved?
If a skimming device was in place when you used a BECU ATM, your name, card number ending in <Last4ofCard>, CVV code, PIN and card expiration date may have been compromised and could be used for fraudulent transactions.

At this time, however, we have **no indication** that your Social Security number, driver's license number or other government-issued ID number, date of birth, address or phone number, or other sensitive personal information or online account credentials have been compromised. As a result, we believe this incident presents a low risk of identity theft.

What we are doing
As an organization, we are committed to ensuring the security of our members' accounts and personal information. The steps we have taken include:

- When BECU first learned of potential skimming events, our team utilized fraud detection technology to help identify and decline potentially fraudulent transactions.
- For those members who reported unauthorized transactions, BECU has reversed those transactions, credited the amount(s) to the affected account and issued a new card. We will continue to support our members in this way if fraudulent activity is discovered.

- BECU ATMs are already equipped with skimming protection that has successfully prevented the insertion of typical skimming devices. And we routinely take steps—and devote significant resources—to increase the security of our ATMs to keep up with industry standards and evolving threats. We will learn from this incident and use the information uncovered during our investigation to further bolster our ATM security.

What you can do

- If you have not already received a new card in connection with this incident, we recommend that you take the following actions:
    - Immediately change the PIN you use with your BECU card. You can easily and quickly do this through Online Banking by visiting the Manage Your Debit Card page. If you use the same PIN for any of your other accounts (e.g., non-BECU financial accounts), we recommend that you change that information as well.
    - Closely review and monitor your account. If you discover any suspicious activity, such as unauthorized transactions, please contact us immediately. You can send a secure message using Messenger in Online Banking or the mobile app, or call a BECU representative at **800-233-2328**.
- If you have already received a new card in connection with this incident, you do not need to take any further action at this time.

Monitor accounts and credit reports

We encourage members to always be vigilant and regularly review and monitor account statements and credit reports, and to promptly report any suspicious activity. You have the right to obtain a copy of your credit report for free once a year 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 following national credit reporting agencies:

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

If you ever suspect that you are the victim of identity theft, please report that 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

For more information

If you have any questions or would like more information about this incident, you can send a secure message using Messenger in Online Banking or the mobile app, or contact a BECU representative at **800-233-2328**, Monday through Friday from 7 am to 7 pm and Saturday 9 am to 1 pm Pacific Time.

We value your trust and membership, and sincerely apologize for this incident and the inconvenience or concern it may cause.

Sincerely,

Ryan Ko
Compliance Privacy Officer