

17236



July 9, 2020

<Name>
<Address Line 1>
<Address Line 2>
<City>, <State> <Zip Code>

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

Dear <Name>,

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?

Beginning in April, BECU received several fraudulent transaction reports from members involving accounts linked to BECU cards. We promptly began investigating these reports and found that all of the affected accounts had been accessed recently by members at certain BECU ATMs.

Based on our continued investigation, we believe that deep insert skimmers were unlawfully installed, and then removed, at six BECU ATM locations in Arlington, Lynnwood, Mill Creek, Renton, and Snohomish, ultimately resulting in the fraudulent transactions.

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. Deep insert skimming devices are more difficult to detect than typical skimming devices because they are generally not visible from the front of the ATM.

The exact dates that skimmers were in place vary by ATM and continue to be investigated. Currently, we believe that skimming devices were in use at the ATMs listed above at some point in April, May, and June 2020. **Our records indicate that you used one of these ATMs during a time frame when a skimmer may have been in use.**

What information was involved?

If a skimming device was in place when you used a BECU ATM, your name, card number, 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:

800-233-2328
becu.org

PO Box 97050
Seattle, WA 98124-9750

- When BECU first learned of potential skimming events, our team deployed 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.
- We are in the process of issuing new cards and PINs to all affected members who have not already received a new card as a result of this incident. We will share additional information with you about this reissue soon. Please watch your mail.
- 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. 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. You can easily and quickly do this through Online Banking by visiting the Manage Your Debit Card page.
 - Closely review and monitor your account. If you discover any suspicious activity, such as unauthorized transactions, please call us immediately 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

If you file a police report, you have a right to obtain a copy of that report.

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

800-233-2328

becu.org

PO Box 97050

Seattle, WA 98124-9750

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

Credit Freezes: Under Massachusetts law, you also 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: credit freezes are designed to prevent potential credit grantors from accessing your credit report without your consent. There is no charge for a credit freeze.

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. To request a credit freeze, 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

At a minimum, you should be prepared to provide the following information in connection with your credit freeze request:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security number, and date of birth;
2. If you have moved in the past five years, the addresses where you have lived over the previous five years;
3. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
4. A legible photocopy of a government-issued ID card;
5. Social security card, pay stub, or IRS Form W-2; and
6. If you are a victim of identity theft, a copy of the police report, investigative report, or complaint to a law enforcement agency concerning the theft.

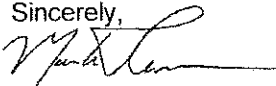
You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

For more information

If you have any questions or would like more information about this incident, please contact a BECU representative at 800-233-2328, Monday through Friday from 7:00 a.m. to 7:00 p.m. and Saturday 9:00 a.m. to 1:00 p.m. Pacific Time.

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

Sincerely,



Mark Thomson
Chief Compliance Officer, Vice President of Compliance and Privacy