WILDWOOD LAW GROUP

3519 NE 15th Ave, Ste 362
Portland, Oregon 97212
www.wildwoodlaw.com
Office: 503.564.3049

Brian T. Sniffen
971.347.1410 direct line
brian.sniffen@wildwoodlaw.com

July 9, 2020

VIA EMAIL AND FIRST CLASS MAIL
(SecurityBreach@atg.wa.gov)

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

Subject: Notice of Data Security Incident

Dear Attorney General Ferguson:

This firm represents Boeing Employees' Credit Union ("BECU"), a Washington state-chartered credit union headquartered in Tukwila. We are writing to notify you, pursuant to RCW § 19.255.010, of a data security incident involving the personal information of approximately 4883 BECU members who are Washington residents. The personal information at issue may include the name, BECU card number, CVV code, PIN, and card expiration date for BECU members.

At this time, there is 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. As a result, BECU believes this incident presents a low risk of identity theft.

Current facts

BECU's investigation is ongoing, but it currently understands the facts as follows:

- Beginning in April, BECU received several fraudulent transaction reports from members involving accounts linked to BECU cards. It 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 its continued investigation, BECU believes that deep insert skimmers were unlawfully installed, and then removed, at 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 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, BECU believes that skimming devices were in use at the ATMs listed above at some point in April, May, and June 2020.

What BECU is doing

As an organization, BECU is committed to ensuring the security of its members' accounts and personal information. The steps BECU has taken include:

- When BECU first learned of potential skimming events, it 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. It will continue to support its members in this way if fraudulent activity is discovered.
- BECU is 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.
- BECU is providing members who used the affected ATMs during the timeframe listed above with written notice in a form substantially as attached (see Exhibit A). BECU's notification letter recommends that members immediately change their PIN (pending issuance of a new card and PIN), regularly monitor account statements and credit reports, and report any suspicious activity via BECU's toll-free number and/or to appropriate state and federal regulatory bodies.
- BECU is notifying its primary regulators, Washington DFI and NCUA, regarding this incident.
- BECU has notified and is cooperating with law enforcement regarding this incident.
- For non-members who used an affected ATM, BECU does not have sufficient contact information for direct contact. It is therefore in the process of notifying the relevant card brands (e.g., Visa, Mastercard) so they may take appropriate steps to reduce the risk to their cardholders.
- BECU ATMs are already equipped with skimming protection that has successfully prevented the insertion of typical skimming devices. And it routinely takes steps—and devotes significant resources—to increase the security of its ATMs to keep up with industry standards and evolving threats. BECU will learn from this incident and use the information uncovered during its investigation to further bolster its ATM security.

BECU values the trust of its members, and it remains committed to protecting the privacy and security of its members' information. If you have any questions, please contact me at (971)347-1410 or brian.sniffen@wildwoodlaw.com.

Best regards,

Brian T. Sniffen

EXHIBIT A

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:

- 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.

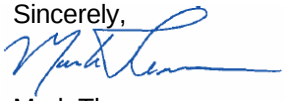
Federal Trade Commission, Consumer Response Center: 600 Pennsylvania Avenue, NW, Washington, DC 20580, 877-IDTHEFT (438-4338), www.ftc.gov/idtheft

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

800-233-2328
becu.org
PO Box 97050
Seattle, WA 98124-9750