FAQS – VISA AND ATM CARD COMPROMISES

BECU may reach out to you either by mail or by phone with information that your current Visa or Mastercard has potentially been compromised. While this call may be unnerving, it is simply BECU taking a proactive stance to protect our members and their finances. Following is a list of the most frequently asked questions that arise when a member is contacted.

What is Skimming?
Skimming is the act of an unauthorized individual obtaining credit or debit card information during the process of a member performing a valid transaction. Typically this occurs during a card present transaction when the card is validly swiped and the information from the black magnetic stripe on the back is compromised.

What is a card compromise?
A card compromise occurs when credit or debit card information is obtained by an unauthorized individual. Most compromises involve a criminal gaining unauthorized access to a merchant's card processor, known as a database/processor intrusion. It can also occur when a suspect is employed at a particular merchant and they are skimming card information at the time of purchase (known as employee skim), or when a skimming device is placed on an ATM machine. In each of these situations, this information is stolen with the intent to commit fraudulent activity.

What personal information is typically stolen and viewable by the suspects when a card is compromised?
When a card is compromised, the suspect typically has access to the card number, expiration date, copy of the magnetic stripe, and/or the three-digit CVV code on the back of your card. Depending on the type of merchant and breach, the cardholder's name, address, and phone number may also be compromised if the merchant was storing this data, but information like address and phone number are not stored on your debit or credit card.

What approach does BECU take when faced with a card compromise?
BECU approaches each card compromise individually. We evaluate the need to reissue debit or credit cards to affected members, and then take the appropriate action based on the present risk.

Does a card compromise mean I have fraud?
Not necessarily. Our goal is to minimize impact however if the risk is deemed high, BECU may take a proactive stance and attempt to block known compromised cards by sending a letter or placing a phone call prior to fraud occurring. In these instances, our goal is to reach out and block the compromised card as a precautionary measure.

What do I do if I discover fraud?
If your card has not yet been blocked, please contact BECU member services at **206-439-5700** or **800-233-2328**. A BECU representative will then block your compromised card, assist with obtaining a new card, review unauthorized activity with you, and submit a fraud notification on your behalf. You will receive reimbursement for unauthorized activity that occurs due to a compromise as long as the activity is reported within 60 days of your statement cutoff date as stated in your account agreement.

FAQS – VISA AND ATM CARD COMPROMISES

How long does it take to receive a replacement card?
All BECU locations have the ability to issue a replacement debit card in person. If convenient, please visit your nearest BECU Neighborhood Financial Center location to obtain a replacement debit card.

If a debit card is to be mailed, the typical turnaround time is 7-10 business days to receive your new debit card as well as your new PIN (Personal Identification Number). Please note that you are able to change this PIN number in BECU Online Banking, at any BECU ATM, or at any BECU location during business hours.

At this time all Visa cards must be sent via mail. This process takes approximately 7-10 business days once the new credit card is ordered.

What if I do not want to have my compromised card blocked?
Fraudulent activity may occur if a compromised card is left active. Having fraud occur can be more of an inconvenience than following the path of having a new card issued. To protect our members and minimize the inconvenience and impact, BECU strongly suggests blocking the compromised card.

What if I have pre-authorized debits or reoccurring payments made to my compromised card?
You will need to contact these merchants upon receipt of your new credit or debit card and provide those merchants with the new card number and expiration date.

What can I do to prevent this from occurring again in the future?
Unfortunately the majority of compromises are unavoidable at the consumer level. It is impossible to predict when your card is going to be compromised so we strongly suggest monitoring your account activity regularly and contacting BECU immediately should there be a transaction that you do not recognize.

Why are details surrounding card compromises kept confidential and not shared with the membership?
At the time BECU identifies or is notified of a potential compromise the investigation is typically in the early stages and the merchant is often unaware they have been compromised. BECU will work directly with Visa, Mastercard, and law enforcement to mitigate the compromise and reduce any outstanding exposure. During this time, details of the compromise are kept confidential to avoid any negative impact to the integrity of the investigation.

What steps does BECU take to monitor for fraudulent activity?
BECU partners with a third party that performs fraud monitoring on our behalf for both Visa and Mastercard. You may receive a call from **888-918-7313**, **727-299-2449**, or **888-241-2440** attempting to verify activity on your account. Please note that this is a valid call and our attempt to contact you regarding suspicious account activity.

Why should I notify BECU if I am planning on traveling?
Please notify BECU if you are planning on traveling. You can do so by calling us at **800-233-2328**, visiting your nearest BECU location, entering travel details in Online Banking Account Services, or by sending a secure message in Online Banking. By notifying BECU of your travel dates and destinations, we can make the necessary adjustments to ensure you are not negatively impacted by our fraud monitoring systems while travelling.