

Compromised Cards Frequently Asked Questions

What is a compromised card?

A compromised card is a card that is at risk of being used fraudulently. Cards may be compromised due to computer theft, unauthorized network intrusion, or any type of suspicious activity.

How does Energy Capital react to compromise notifications?

ECCU takes every compromise seriously and requires issuance of replacement cards for affected members. Members will receive written notification if their card data has been compromised. Replacement cards & pin will be issued on the date of the notification letter and the old compromised card will be blocked 10 business days from when the replacement card was issued.

What if a fraudulent transaction clears my account and I do not have enough money to pay my bills?

ECCU will issue you a provisional credit within 10 business days while this matter is being disputed with Mastercard. Then, ECCU receives credit back when the matter is resolved.

How long will it take to receive my replacement card?

Most cards are received within 2 weeks from the date of the order. The new PIN is delivered two or three days after that.

What happens if I do not receive my card by this time?

Please contact ECCU at 832-604-4848 so that we can check on this immediately.

What if I do not want to have my card blocked?

Compromises are serious. Fraudulent activity may occur if the card is not blocked. The fraud dispute process can be more inconvenient to members than simply having a card replaced. While many members do not experience fraud when a compromise is reported, the risk exposure still exists if the cards are not blocked and replaced. To protect our members, minimize inconvenience and losses, Energy Capital Credit Union requires compromised cards to be replaced.

Does this mean that I have fraud on my account?

Not necessarily. In fact, among the list of card numbers we periodically receive, only a few are affected by fraud. Take the opportunity to review your monthly statement(s). Remember to view your current transaction history using Virtual Banking.

What do I do if I discover fraud on my account?

Contact Vanity immediately. For Debit Card transactions, call 1-800-808-6402. For Credit Card disputes call 1-800-600-5249.

What if I have preauthorized debits made to the compromised card number?

You should contact the merchant(s) immediately upon receipt of your replacement card(s) and provide them with the new card number and expiration date. This process may be as simple as logging into the corresponding merchant(s) site and updating the information. If this is not the case, you may need to write to them to let them know of a card number change.

There are other authorized users on my Debit or Credit Card account. Does this affect their cards too?

Debit cards each have a separate number. Therefore, if one card is compromised, that doesn't always mean the authorized user card is compromised as well. Credit cards have the same number, so both cards have to be replaced immediately.

Can this information be used to steal my identity?

The information encoded on the compromised card pertains strictly to the card, potentially including the card number and expiration date. Confidential information such as Social Security Numbers, driver's license numbers, addresses and dates of birth are not stored on the card.

What can I do to keep this from re-occurring?

Unfortunately, we have no way of stopping criminals from "hacking" into databases of merchants. While the possibility of a card being used fraudulently is low, we recognize the aggravation members face in acquiring a replacement card or to have fraudulent activity removed from their account.

Is there anything I can do to ensure that fraud doesn't occur on the card?

Always know where your card is, and if you misplace it, contact us immediately so we can block the card from use. Never write their PIN on the card or carry the written PIN with you. Use virtual banking to monitor your account activity and contact us if you see anything suspicious.