BPC Card Security

Card Security Features

In an effort to minimize the threat of fraudulent activity and to help protect the University, the following security measures have been incorporated into the BPC card program:

1. The card's Expiration Date and CVV code
2. Maximum preset "monthly credit limit" authorized for your account
3. Maximum preset "per transaction" dollar limit authorized for your account
4. Additional overrides are required for the following situations:
    a. Purchases over $5,000
    b. International Purchases
    c. Declines due to unapproved MCC code

As an Accountholder, it is your responsibility to keep your credit card information secure. The following are some high risk area's to be mindful of:

- Account numbers must be safeguarded against usage by unauthorized individuals in the same manner you would secure your own personal credit card
- Transmitting complete credit card information electronically via fax or regular email is not allowed. Dropbox is a University acceptable form of transmitting your credit card information securely.
- In a non-secure environment, it is recommended that you only provide the last four digits of the account number and request the vendor contact you by phone to provide the remaining account information
- Credit card information given over the phone. Know who you are doing business with before placing an order.

It is highly recommended that the Accountholder log on to the bank's website (www.commercialcardcenter.com) periodically throughout the statement cycle period to review their account activity. Contact the BPC Administrator immediately if you suspect fraud or abuse.