Published on *University of Colorado* (https://www.cu.edu)

Fraud Doesn’t Take a Vacation – Keep Your Commercial Card Safe This Summer [1]

June 3, 2025 by Staff [2]

As summer approaches – whether you're wrapping up year-end purchases, booking travel, or taking some well-earned time off – remember that scammers don’t take vacations. In fact, this season can be prime time for fraudsters targeting distracted cardholders. If you have a university-issued Procurement or Travel Card, here are the current fraud trends to watch for and tips for keeping your card secure.

Wanting to know the single most important safeguard? Regularly monitoring your charges in Concur.

Phishing Emails and Texts (Smishing)

- Scammers pose as banks, credit card providers, or even CU employees to trick you into clicking malicious links or sharing sensitive information
- Messages often look urgent or reference "issues” with your card or payment
- Call the number on the back of your card if unsure, do not call any number found in the message
- No bank rep or PSC staff member will ever ask for your full card number

Business Email Compromise (BEC)

- Fraudsters impersonate suppliers, supervisors, or colleagues asking you to make purchases or change payment details
- Messages may appear legitimate with real names used
- Always verify by contacting the person or supplier directly using contact info outside the message (e.g., Teams for CU or via the supplier’s official site)
- Never act on unsolicited emails requesting payment details

Fake Travel Booking Sites

- Beware of fraudulent travel booking sites that steal credit card data
- CU employees should book travel through Concur or directly with Christopherson Business Travel

Subscription Traps

- “Free” or low-cost subscriptions often lead to unauthorized recurring charges
- Especially common with software or publications
- Follow proper procurement procedures, especially for software, which should not typically be purchased with a commercial card

- Always review your monthly charges for accuracy

Card Sharing

- Do not share your physical card nor your 16-digit card number with others, not even other employees
- Card-sharing can lead to unexpected or unauthorized transactions
- Cardholders are responsible for misuse that results from unauthorized card-sharing

As a university commercial cardholder, you are the first like of defense in protecting CU's financial resources. If you notice suspicious activity, contact the bank immediately using the number found on the back of your card. For help verifying a suspicious message, contact your campus IT team or the sending organization using official contact methods. For card related support, reach out to PSC@cu.edu [3].

Travel and Expense [4]
Send email when Published:
Yes

Links
[1] https://www.cu.edu/blog/psc-communicator/fraud-doesn%E2%80%99t-take-vacation-%E2%80%93-keep-your-commercial-card-safe-summer [2] https://www.cu.edu/blog/psc-communicator/author/69272
[3] mailto:PSC@cu.edu [4] https://www.cu.edu/blog/psc-communicator/tag/travel-and-expense