Everyone at UT is Responsible for Credit Card Security

Everyone at the University of Tennessee has a part to play in combating credit card fraud. No one wants to be the victim of credit card fraud, so we all have to work together to keep cardholder data safe.

Countless credit card transactions are processed by UT merchants every year. Customers expect us to safeguard their financial identity and there are severe consequences for the University if we do not. In order to secure this vital information from fraud, theft, and abuse, a few basic guidelines must be followed.

If your department accepts credit or debit cards, here are a few ways to help combat fraud:

1. Protect the cardholder data at all times.
2. Do not write down or share cardholder data unless it is part of the approved and documented business process.
3. If you must store any documents that contain cardholder data, ensure the primary account number, CVV/CVC, and PIN are redacted.
4. Secure any cardholder data in a safely locked location.
5. Destroy cardholder data as soon as your business process and legal requirements allow.
6. Do not request cardholder data via end-user messaging technologies, such as email, text, or instant message. If received, delete the data immediately and contact the customer.
7. Document, review, and regularly update your credit card processing policies and verify that everyone is aware of their responsibilities.

In addition to following these guidelines, confirm that all employees involved with credit card processing are familiar with the departmental policies and procedures, as well as UT’s FI0311 – Credit Card Processing.

If you have questions about credit card security, please contact your campus business office, the Treasurer’s Office, or the UTSA Information Security Office.