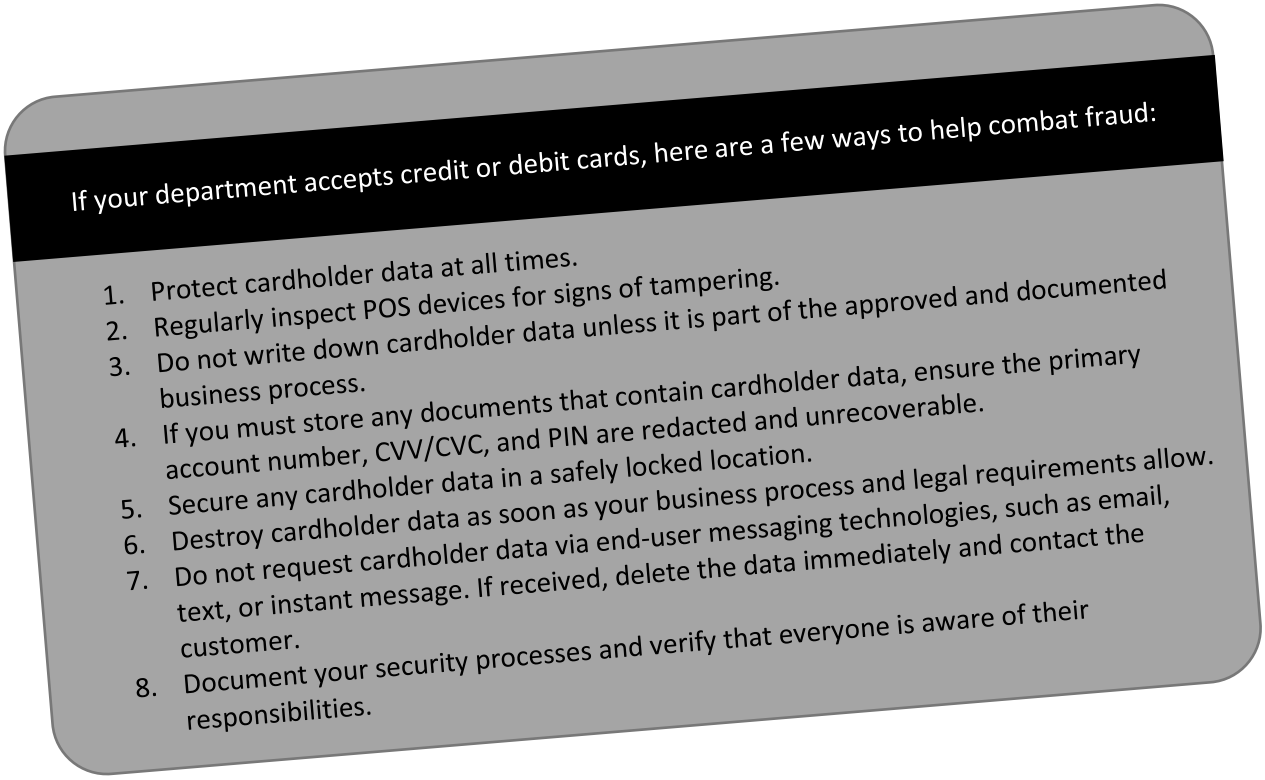
Responsibility for Credit Card Security

If you process credit card transactions at the University of Tennessee, you have a direct role in combating credit card fraud. We must all work together to keep cardholder data safe. Remember that cardholder data is, at a minimum, the full primary account number (PAN), but may also be the full PAN, plus any of the following: cardholder name, expiration date, and/or service code.

UT merchants process hundreds of thousands of credit card transactions 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.



In addition to following these guidelines, please review departmental credit card processing policies and procedures at least annually and update as needed. Confirm that all employees involved with credit card processing have completed the required training and 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.