

Cardholder Data

The Payment Card Industry Data Security Council defines **cardholder data** as follows:

Full credit card number, also known as the [Primary Account Number \(PAN\)](#), plus any of the following:

1. Cardholder name
2. Expiration date
3. Service (Security) code

The University does not permit the storage of the codes found on the magnetic strip, Personal Identification Number (PIN), encrypted PIN block, or the card validation code (three digit code on back of credit card or four digit code on front of American Express card) under any circumstance.

The complete credit card number is always considered cardholder data. Any time the complete credit card number is present, the cardholder name, expiration date and service code are also considered cardholder data.

PANs are never to be sent via end-user messaging technologies (i.e. email, SMS, etc.).

The last four digits of the credit card number may be maintained for reference and do not constitute cardholder data. Customer receipts should not show more than the last four digits of the credit card number. Computer systems and software used to process credit card transactions should not display more than the last four digits of the credit card number.

All employees that have access to cardholder data must keep this information in the strictest confidence, and protect it from unauthorized access or disclosure. Access to this information should be on a need-to-know basis only.

Prior approval must be obtained by Information Technology Services (ITS) for the use of any hardware, software, electronic system, or external entity used to process credit card transactions.

Ideally, areas within the University that accept credit card transactions will not have a need to write down the customer's credit card number. However, there are circumstances where the credit card number must be temporarily written down, and we then have a document containing cardholder data. These documents contain extremely sensitive data and should be kept physically secure, and safeguarded at all times. Please refer to the [Procedure for Paper Documents Containing Cardholder Information](#) for an outline of the minimum requirements related to these documents.

Questions/ Concerns:

Matt Packard, CCEP

Chief Compliance Officer

850.857.6070 | mpackard@uwf.edu