

# CYBER SECURITY

## newsletter

### PCI DSS

#### Problem

Credit cards have become the primary way many people make purchases, especially with the growth of online shopping. Credit cards are incredibly convenient, they allow you to make very large purchases almost anywhere in the world, simply by having a card. In addition credit cards can be safer than carrying cash, if you lose your credit card you simply call your credit card company and cancel the card. If you lose your cash, it is gone forever.

However, credit cards also have a risk. Cyber criminals are actively trying to steal credit card information. If they steal your credit card data, they can create physical copies of your credit card, or simply use the information for online purchases. The more credit cards criminals steal, the more money they can make. As a result, many criminals no longer target individuals but organizations that store, process or transfer cardholder data. Since our organization has such data, we are a target for criminals.

#### Solution

To reduce credit card fraud, five members of the payment card industry, Visa, Master Card, American Express, Discover and JCB, joined together to develop security standards for any organization that stores, transmits or processes credit card data. This set of standards is referred to as the Payment Card Industry's Data Security Standard, or "PCI DSS." Since our organization handles such data, we must understand and abide by these rules.

Cardholder data is defined as the credit card number (sometimes called a PAN) and any associated information, such as expiration date, name, address, telephone number, card validation code, or any other cardholder's information. PCI DSS details how we must protect this information so criminals cannot steal it. If criminals gain access to our cardholder data, potentially millions of people can be affected. In addition, we can be liable for damages. By following these rules, you help ensure our organization is both secure and compliant.



#### Protecting Cardholder Data

*Since our organization handles cardholder data, we have to understand and follow the security regulations known as PCI DSS. This newsletter explains what those standards are and how we must follow them.*



University of Colorado

Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to [security@cu.edu](mailto:security@cu.edu) or visit <https://www.cu.edu/information-privacy-and-security>

# Examples of Cardholder Data

*There is a variety of different types of information that can make up cardholder data. Specifically, it is any information that is the combination of the credit card number (or PAN, Primary Account Number) and any other related information. For the example we have to the right, the credit card number (or PAN) is*

5490 2345 8670 8921

*Other types of data that would be considered cardholder data, when combined with this would include*

- The card holder's name.
- The cardholder's billing address.
- The cardholder's telephone number.
- The card's expiration date.
- The card's security code. This is a three or four digit value written usually on the back (but sometimes on the front of the card). This number can be called the CSC, CVD, CVC, or even CVV2 value. In the example to the right, the card's security code is 239.
- The card's PIN. This number should not be confused with the PAN. PIN is the cardholder's password entered at the time of transaction and should never be recorded, printed or stored.

**1. Authorized Systems.** You must use only authorized payment systems to enter, process or store cardholder data. Do not copy or store cardholder data to any unauthorized systems, such as personal mobile phones, laptops or USB sticks.

**2. Authorized Personnel.** Only share cardholder data with authorized personnel who have a need to know.

**3. Acceptable Use:** Payment systems may only be used for processing payments, do not use them for non work related or unauthorized activities, such as surfing the web, reading email or chatting with someone online.

**4. Storing Data:** The storing of any authentication information such as the users PIN or full details of the credit card track is expressly prohibited. In addition, the credit card number should not be stored if at all possible. If it is stored it must be encrypted with proper key management and masked if displayed on a computer monitor or paper printout.

**5. Transfer:** If you transfer cardholder data you must use encrypted methods that are approved by our organization.

**6. Data Destruction:** All physical and electronic cardholder data that is no longer necessary or appropriate to store must be properly destroyed, shredded or rendered unreadable.

