

Basics of Securing Credit Card Data

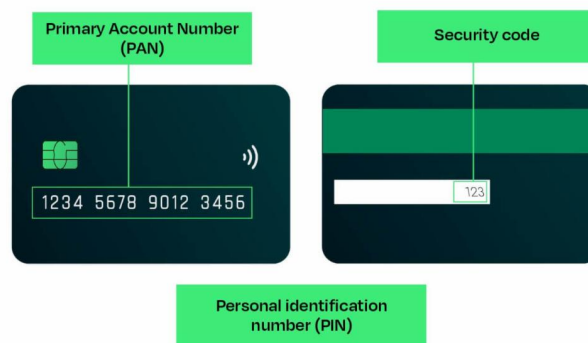


Cybercriminals often focus on getting access to payment and credit card data due to potential financial gains. It might take only a mistake to put this type of data at risk.

Anyone who handles credit cards and/or credit card data should understand the best practices for keeping this valuable information safe.

Cardholder Data

This is the most sensitive credit card information and thus the most valuable to bad actors.



Visit the **Protecting Customer Credit Card Data** Lesson only course to learn more.

**Get Started
Now**

Simple Rules for Handling Credit Card Data

1. Emails

Never send emails or other correspondence containing full credit card information..



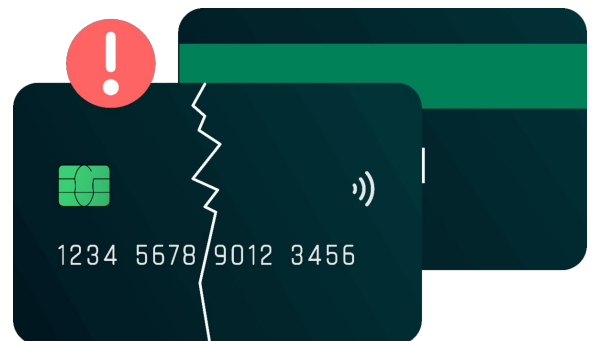
2.

Credit card numbers

Avoid physically writing down credit card numbers.

3. Physical and electronic cardholder data

Physical and electronic cardholder data must be destroyed after it is no longer needed.



4.



Suspicious activity

If you see any suspicious activity or are uncertain about, report it!

**Thank you for your support in
keeping Billtrust safe!**

If you have any questions, email
security@billtrust.com.



Billtrust | 1009 Lenox Drive, Suite 101, Lawrenceville, NJ 08648

[Unsubscribe cshaw@billtrust.com](mailto:cshaw@billtrust.com)

[Update Profile](#) | [Constant Contact Data
Notice](#)

Sent by bydfong@billtrust.com powered by

