Card-Not-Present Transactions

A Card-Not-Present (CNP) transaction is a transaction where the physical credit or debit card is not present. Instead, the customer provides their card details remotely (online, by phone, etc.), and the merchant processes the payment without physically interacting with the card.

Examples of Card-Not-Present Transactions

- **Online Purchases:** When shopping on e-commerce websites, customers enter their card details (credit card number, expiration date, and CVV) to complete the purchase.
- **Phone Orders:** Customers call a business to place an order and provide their card information over the phone to complete the transaction.
- **Subscription Services:** Signing up for a subscription service (like Netflix or Spotify) where the customer enters card details for automatic billing.

Pros of Card-Not-Present Transactions

- **Convenience:** CNP transactions are often more convenient for both customers and merchants. Customers don't need to be physically present to make a purchase, and merchants can serve a broader market, including international customers.
- **24/7 Availability:** Since CNP transactions can occur online or through other channels, they allow businesses to operate beyond regular store hours, enabling sales and transactions at any time.
- **Global Reach:** Merchants can reach customers anywhere in the world without needing a physical location, which is especially beneficial for e-commerce businesses.

Cons of Card-Not-Present Transactions

- **Higher Risk of Fraud:** Since the card is not physically present, CNP transactions are considered more vulnerable to fraud.
- **Higher Risk of Chargebacks:** CNP transactions are more susceptible to chargebacks, where customers dispute a charge, often leading to the merchant losing both the product and the payment.

Card-Not-Present Transactions

Best Practices for Card-Not-Present Transactions

- Make the customer aware of your business. Post significant identification for the customer to easily identify your business.
- Never write down (or type) customers' credit card numbers.
- Never photocopy, or imprint, customers' payment cards for later use.
- Obtain authorization from customers to store card information.
- Request a copy of the customer's ID if possible.
- Use the Address Verification System (AVS). Require the billing and shipping address match.
- If goods are being shipped, require a signature at delivery.
- Implement extra security measures like CVV (Card Verification Value) checks.
- Offer two-factor authentication at login and add CAPTCHA to mitigate fraud risk.