



From the

Heartland Newsroom

Insights, articles and news
HeartlandPaymentSystems.com

Reduce the Risk of Fraud on Card-Not-Present Transactions

By P. Gayle Hoskinson, Interchange and Compliance Manager
Mike Hall, Loss Prevention Manager
Heartland Payment Systems™

Does your business accept “card-not-present” payments — payments made by phone, internet or mail? If so, you might be at increased risk for payment card fraud. There are some red-flag signs that card-not-present transactions could be fraudulent. They include requests for overnight shipping, transactions placed on multiple cards but shipped to a single address and orders that include large quantities of the same item. Indicators like these should prompt you to follow up and check on the order. (See the sidebar “Potential Signs of Card-Not-Present Fraud” for more indicators of possible fraud.)

In addition to knowing the warning signs, take these steps to reduce your risk of accepting fraudulent transactions:

1. Obtain a proper authorization to verify the credit card has sufficient funds available to cover the transaction amount. Ask the customer for the card expiration date, and include this in the authorization request.
2. Call the customer back and ask him/her to verify the transaction information.
3. Participate in cardholder verification programs like Address Verification Service (AVS). AVS automatically compares the customer’s address with the billing address on file with the card issuer.
4. Use cardholder verification programs like Visa’s Card Verification Value (CVV), MasterCard’s Card Validation Code (CVC) and the Card Identification Number (CID) from Discover and American Express to validate the cardholder. This is a three-digit code printed on the back of Visa, MasterCard and Discover cards — and a four-digit number on the front of an American Express card. This code enables you to verify the buyer has the card on hand during a card-not-present transaction. You should ask the customer for his/her verification code and enter it into your terminal or POS system so it will be sent to the card issuer as part of the authorization request.

Following these simple steps and knowing the potential signs of card-not-present fraud can save you time, frustration and money so you can focus on what really matters ... growing and improving your business.

Potential Signs of Card-Not-Present Fraud

Keep on the lookout for these warning signs of potentially fraudulent transactions:

- Larger-than-normal orders
- Orders that include several of the same item
- Orders made up of “big-ticket” items
- “Rush” or “overnight” shipping
- Shipping to an international address
- Transactions with similar account numbers
- Shipping to a single address, but transactions placed on multiple cards
- Multiple transactions on one card over a short period of time
- Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses
- For online transactions, multiple cards used from a single Internet Protocol (IP) address



P. Gayle Hoskinson is manager of interchange and compliance and Mike Hall is manager of loss prevention at Heartland Payment Systems. Heartland, a NYSE company trading under the symbol HPY, delivers credit/debit/prepaid card processing, payroll, check management and payment solutions to more than 250,000 businesses nationwide.

Heartland is the founding supporter of The Merchant Bill of Rights, a public advocacy initiative that educates merchants about fair credit and debit card processing practices. For more information, contact Heartland Payment Systems at 866.941.1HPS or visit HeartlandPaymentSystems.com and MerchantBillOfRights.com.