BEST PRACTICES WHEN CARD NOT PRESENT E-COMMERCE

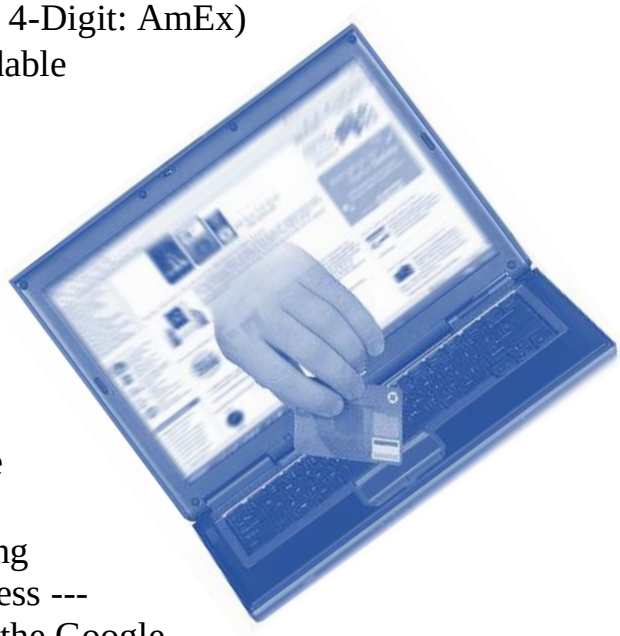
Best Practices – When Card Not Present

In today's modern age, a great majority of all business interactions are done online, whether you are the consumer or the provider. From the provider's standpoint, it is wise to protect our business from the ever increasing instances of fraudulent transactions in our online/ ecommerce society. Below you will find useful information to help merchants avoid becoming a victim of these fraudulent transactions. The more you know, the more you will be able to recognize any fraudulent attempts and in the end be more Productive!

What to make sure you have confirmed

If you accept transactions over the phone or via the internet, you should make sure that you have the following card information confirmed:

- Account Number or Credit Card number
- Name as it appears on the card
- AVS: Address Verification of the Billing Address and Zip Code associated with that card
- CVV (3-Digit: VISA, MasterCard, & Discover and 4-Digit: AmEx)
- ***MAKE SURE TO ALSO OBTAIN***: Clear and Readable copies (ID's, proof of credit card, etc.)



Verification

When verifying the cardholders issuing bank, there are a few things to keep in mind:

- NEVER call the 800# on the back of the card (If it is a fraudulent card, the 800# will be a fake too)
- Go to State driver's license *.gov* website to view the state IDs to compare the ID presented to you
- Google Maps – Cross reference the purchasers billing address that is provided as well as the delivery address --- If delivery is to supposed to ship to a residence and the Google map reflects a warehouse … Beware!!
- Social Media – Almost everyone is on social media, if you believe the customer/client transaction to be suspicious, you can try to "Google" the person and may be likely that you will find the "actual" person on a social media site for more verification.

E-COMMERCE BEST PRACTICES

- Use a Secure Gateway "*https*:" (E-Commerce)
- Use Fraud Controls: Fraud Protection
- DO NOT ship to freight forwarding companies
- Delay Delivery **Do not ship your product for the first 48 hrs after purchase. This allows time for credit card owners to see the purchase on their billing. If it is a fraudulent transaction, the credit card owner now has time to stop the transaction from completing.
- Make sure you are PCI and EMV compliant every year
- Select the right processor to assist with Chargebacks.
- When shipping with FedEx or UPS: (Most secure way to avoid delivering to a fraudulent person):
  Send every item marked as *SIGNATURE REQUIRED – DIRECT SIGNATURE*** this will ensure that the actual person who has purchased the product (name on credit card) is the person who is receiving and signing for the product. The delivery drivers will be required to ask for an ID – if the person that is receiving is not the original purchaser of the product – the driver will ask for proof of residence (where the product is being delivered) and/or an ID with the matching last name.
- Keep record of previous disputes or chargebacks and the delivery addresses.
- You can add Verified by Visa and MasterCard SecureCard for more levels of protection (Customers can add this)

As the business owner, you must always keep one rule in mind, if it seems ***Too Good To Be True***, then it probably is. If you notice a larger than normal purchase, make sure to follow all of the steps above to help protect yourself from fraudsters.

Key Terms:

- AVS

The Address Verification System (AVS) is a system used to verify the billing address of a credit card holder. The system will validate the billing address of the credit card provided with the address on file at the issuing credit card company.

- CVV

The CVV number (Card Verification Value) on a credit card is a 3-4 digit number on VISA, MasterCard, Discover, and American Express credit cards

Aliant Fraud Protection Features

Below are fraud prevention tools and features that, when used appropriately, can help you to secure your transactions and in the end secure your business:

- Thresholds: Allows you to set parameters of your fraud protection. You can create Rules and restrict certain IP user. Set volume limitations, transaction times, rules for failed attempts, etc.
- User Ban: Allows you to ban a specific user, ban the IP address (or several IPs), and filter our credit card numbers, country, or even user information.
- Set Up Exceptions: Allows you to permit "Known good users" that would not pass any restrictions that you have placed but that are valid users. (you know them to be legitimate)
- Set Up a Waiting Review Cue: Allows you to review suspicious transactions. Also allows you to cancel the potentially fraudulent charges that were submitted by logging in to your gateway account.
- Review your History Logs: Allows you to see recent transactions and track fraudulent attempts.

As a merchant processor, we see the back end and the dangers of chargebacks and fraudulent charges. Always secure your business with the best, knowledge!

About Aliant Payment Solutions

Aliant is a merchant services company that provides debit card and credit card processing to small, medium and enterprise businesses. To learn more about Aliant Payment Systems, visit *http://www.aliantpayments.com*.