

## **Consumer Fraud Scams**

### **How to Protect Your Business**

Employee training can be very important, especially when it comes to processing Credit Cards. Many business owners have dealt with Chargebacks due to fraudulent purchases. However, these can often be avoided by training all employees in proper procedures at the point of sale.

A recent scam that has caused merchants to lose thousands of dollars could be avoided by proper training. Here is the scam:

A customer will go into an establishment with a cancelled card and attempts to make a large purchase. The merchant runs the card and gets a "DO NOT HONOR" message on the terminal or software. The customer then tells the merchant or employee that there is a mistake and asks if he/she can use the phone to call the bank number on the back of the credit card.

The customer doesn't really call the bank, but instead calls an accomplice posing as an associate of the issuing bank. The customer then hands the phone to the merchant. Next, the imposter on the phone asks the merchant to read the cardholder name, credit card number and expiration date. Then the phony bank agent gives the merchant a bogus approval number and walks the merchant through an offline transaction on the terminal or Point-of-Sale device.

The terminal will take the transaction with the fake approval number and issues a receipt. The real Issuing Bank will chargeback the funds because the transaction was not legitimate and the merchant loses the money.

This scam has been very prevalent in New England, especially at liquor stores. Here are some steps to take to ensure you're processing legitimate transactions:

- Every merchant account has a Voice Authorization line that should be dialed and processed in full by the merchant. Most are automated systems that will immediately ask for a Merchant ID Number. Most Voice Authorization Centers offer Operator Assistance.
- If you receive a "Do Not Honor" message, it is your responsibility to call your Voice Authorization center for proper Authorization. If the Authorization Center also replies with a "Do Not Honor" message, then the sale should be rejected. It is not a valid practice for a merchant to get an Authorization Code from an issuing bank number that is on the back of a credit card.
- ALWAYS imprint any card that does not process with the magnetic strip.
- When in doubt, if you do not know your customer, reject the sale or ask for another form of payment. Also, beware of anyone wanting to put a purchase on two different credit cards.

- Do not process a sale using a card that clearly has a different name than that of the person presenting the card (e.g., a man using a woman's card).
- Beware of those who claim "My father gave me his card because I am in college" or "My wife took my card by mistake and I am using hers". Merchants have the right to reject any payment that is not presented by the actual cardholder.

For more information on how to protect your business from fraud, visit the Visa USA website link below:

[http://usa.visa.com/download/business/accepting\\_visas/ops\\_risk\\_management/merchant\\_catalog.pdf](http://usa.visa.com/download/business/accepting_visas/ops_risk_management/merchant_catalog.pdf)