More Mileage, Less Risk
Filling up on point-of-sale perfection
As a convenience store or other petroleum retailer, you have specific needs at both the pump and the point of sale that differentiate your business from other retail markets.

According to the National Association of Convenience Stores, U.S.-based locations reached record in-store sales in 2013, with motor fuel sales of $491.5 billion. Transactions at the pump came from approximately 106,000 stores nationwide.¹ Their explicit needs include strong support after boarding, exceptional customer service, reporting capabilities and reliable relationship management. In addition, you handle working relationships with your own clients, such as industry associations and fleet companies. Given these business challenges that fuel petroleum merchants every time a car pulls in, speed, reliability and efficiency must be embedded in your payment processing solutions.

From the moment a customer swipes a card at the pump, the transmission of sensitive data begins and your information security measures are tested. As new locations are established, the chances of a data breach are greater among thousands of customers within the parameters of your franchise. With all of this risk accompanying the point of sale, what premium practices should your business run on without taking your time away from customers?

First, make sure your processing system includes:

- Acceptance of all major credit cards
- Acceptance of major fleet cards
- Current technology on the market to process your purchases
- Quick and easy payment acceptance for your on-the-go customers
- Low processing fees that give you higher return.

In addition, innovative reporting solutions that provide a strong tracking and analytics backbone for your long-term strategy and planning, loyalty programs and ability to void transactions efficiently are all important.

Once you have enlisted your payment processor to ensure that your processing solution offers these capabilities, go the extra mile to safeguard your business by implementing and understanding the following fraud prevention tools:

**Payment Card Industry Data Security Standard (PCI DSS) Compliance**

Perhaps the most significant requirement to prevent fraud occurrences is the Payment Card Industry Data Security Standard (often shortened to "PCI DSS"), a set of data security requirements established by the major card organizations to protect cardholder account information. Anyone who accepts debit and credit card transactions must be compliant with the following 12 requirements at all times:

1. Build and maintain a secure network. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Maintain a vulnerability management program. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Implement strong access control measures.
8. Restrict access to cardholder data by business need-to-know. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Regularly monitor and test networks. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain an information security policy for employees and contractors.

**Address Verification Service (AVS)**

AVS is a service that is required to be used on all card-not-present (keyed) credit card transactions. In the case of petroleum merchants, AVS highly recommends that the customer enter the zip code at the time of transaction. When that transaction is submitted for authorization, the zip code entered is checked against the actual billing zip code for the cardholder. The AVS response provided by the issuing bank either indicates it is a match, partial match, no match, or AVS not available or error.
Rapid Report

If your company has experienced a suspected or confirmed security breach, take prompt action.

1. Immediately contain and limit the exposure.

2. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information.

3. If compromised, you should consult with your internal incident response team. To preserve evidence and facilitate the investigation, immediately alert all necessary parties, which would include your internal incident response team and information security group, Bank of America Merchant Services Initial Response Team at 1.800.228.5882, and the appropriate law enforcement agency.

On the road with bumper-to-bumper competitors, there’s more than one way to provide exceptional customer service, manage relationships with associations and other industry resources and remain speedy. While driving your business to the top, don’t forget to reinforce your card acceptance policies with best practices that secure your transactions.


© 2014 Banc of America Merchant Services, LLC. All Rights Reserved. All trademarks, service marks and trade names referenced in this material are the property of their respective owners. Merchant Services are provided by Bank of America, N.A. and its representative Banc of America Merchant Services, LLC. Banc of America Merchant Services, LLC is not a bank, does not offer bank deposits, and its services are not guaranteed or insured by the FDIC or any other governmental agency.