Preventing fraud

Credit-card fraud involving illegal gas trucks is on the rise. It’s not a new trend, but it’s one that’s more popular as gas prices rise.

The scam works as follows: The bed of a pickup truck or back of a van is converted into a 300- to 500-gallon gas tank. The scammers then use stolen credit cards to fill the illegal tank. A switch is installed under the driver’s seat that opens the factory-installed fuel tank and allows the contents to be transferred into the converted tank.

The offenders sell the gas on the streets, or sell the entire truckload to one of your competitors. Imagine your hard-earned, quality gas that you purchased being sold to your low-price competitor across the street, who’s in turn selling it to his customers.

You can do a few things. First, talk to your employees, especially on the night shift. They can see when one truck is taking more than half an hour to fill up. If they see this happening, they should call the police. (Unfortunately, often they’ve been offered $100 to look the other way.)

Second, do night rides. Visit your stores to surprise your employees. If they know you spot-check, they might be less likely to be bought off.

Third, check your credit-card sales at the pump. If you see an unusually high spike one night, you may have been hit. Call in the employee who was working to see what they know.

Another risk

The most popular form of credit-card fraud is skimming. You have a much greater chance of being a victim of skimming—and it could put you out of business. Essentially it involves stealing a customer’s credit-card mag-stripe data without the customer ever knowing.

Why are our stations great targets for skimming?

- They have a high volume of credit-card activity.
- Employees often work alone, or with no supervisor.
- Employees are easily compromised.

With skimming, criminals will make your cashier an offer that’s hard to refuse. They’re given a skimmer, which looks like a pager, and asked to swipe every credit card on their shift through the skimmer. The pager steals and stores your customers’ mag-stripe data, which is then transferred to another credit card for use, and the customers have no idea because they still have their cards.

At the end of their shift the cashier is given $100 to $200 for each card they swiped. You can do the math and see how attractive this is to a cashier who’s already working overtime and/or other jobs. Not bad for one night’s work.

Operators are responsible for protecting their customers’ mag-stripe data; it’s in the credit-card agreement with the card issuers. So all the fraudulent purchases made with those card numbers, which were compromised at your store, could be charged back to you. We’re responsible for employee actions, just like the prevention of the sale of cigarettes and alcohol to minors.

In some cases skimming is the reason why people work at service stations. Hint: When you have someone willing to drive a long way to work, loves the night or graveyard shift and overtime, it’s not a dream come true—it’s a clue.

Linda McKenna is principal and co-founder of Employee Performance Strategies Inc. (EPS), Chantilly, Va. (www.eps-icom). EPS helps clients increase their competitive advantage and profitability through people. McKenna provides keynotes and leadership seminars for businesses and associations. McKenna’s industry commentary appears exclusively in CSP.