FRAUD: THE HIDDEN COST OF FLEET FUELING

Contents:

EXECUTIVE SUMMARY

Fuel is the single largest expense facing commercial fleet operators. A recent Havill & Company industry study found that 18 percent of fleet managers have experienced fraud or misuse. The problem is even more widespread when you consider the abuse that has gone undetected.

Management is responsible for safeguarding company resources and there are many tools for achieving this goal. The first priority must be to manage this risk by removing opportunities for these losses to occur. Here, purchase restrictions, such as fuel only cards, and lockouts, such as time-of-day and day-of-week authorization apply.

Next, the fleet administrator needs a robust reporting system that monitors fuel consumption and flags exceptions requiring further research. When fraud is detected, management must be able to quickly take away purchasing privileges. When cards are used, this means instantaneous card lockouts.

Unfortunately, many fleets are using fuel payment programs that do not offer the needed protections against fraud and misuse; and when these security features are available they are frequently not used.

This white paper details the risks facing today's fleet administrator and the tools available to manage these risks. When a typical 100 vehicle fleet spends $30,000 per month for fuel, the added cost of fraud and misuse is too important to ignore.

ABOUT HAVILL & COMPANY

Havill & Company publishes the multi-client study series entitled: *The U.S. Commercial Fleet Market Forecast, 2004-2008.* It is respected as the primary source for planning data among the leading vehicle manufacturers, leasing companies, major oil companies, fleet card providers, and maintenance and TBA suppliers.

Havill & Company was founded in 1987 as a full service B2B market research and management consulting firm. In 2002, the company launched the www.FleetLeads.com website to enable its clients to more effectively market their products and services to commercial fleet operators.

Fraud: The Hidden Cost of Fleet Fueling

The typical organization loses an estimated 6 percent of its annual revenues to occupational fraud, according to research conducted by the Association of Certified Fraud Examiners. If this is multiplied by 2004 U.S. gross domestic product, which was over $11.7 trillion, it would translate into $704 billion in annual fraud losses. Without question, this is a staggering amount of money.

According to the National Association of Convenience Stores, in 2004, fuel thefts cost retailers in the U.S. $237 million dollars, more than twice the $112 million lost in 2003.

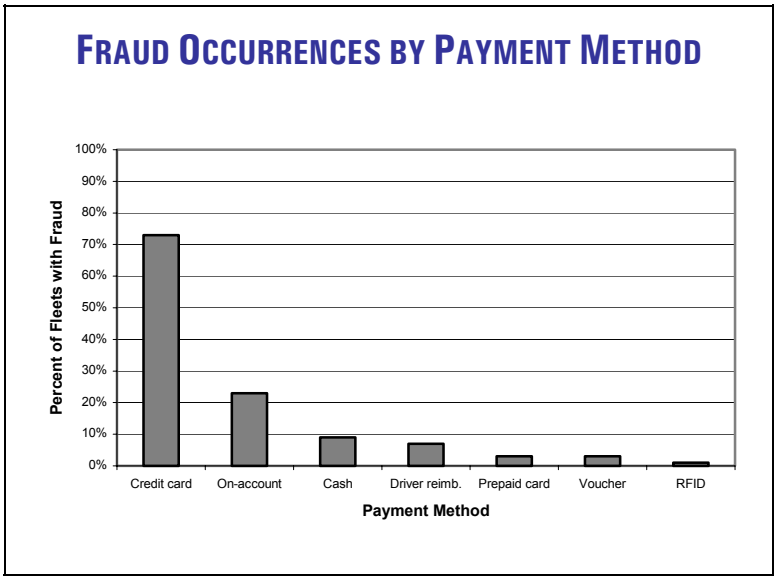
Vehicle fueling is particularly susceptible to fraud because it is a difficult activity to supervise. Over the past year, gas stations across the nation have seen an increase in the number of drivers filling up their tanks and leaving without paying. Company employees have also felt the squeeze of high fuel prices, and for some, the temptation to abuse their fueling privileges is too great to pass up.

Fuel is the single largest expense for commercial vehicle fleets. A typical 100 vehicle fleet can easily spend $30,000 per month to fuel its delivery vehicles and sedans. Someone at the company must account for an expenditure this large.

Unfortunately, many companies lack the controls to protect the moneys going to fleet fueling. This shortcoming was revealed in a recent industry study conducted by Havill & Company. A survey of over 1,100 fleet operators nationwide found that 18 percent of these companies had fallen victim to fueling fraud or misuse.

Fraud was not confined to only one payment method.

Fraud Occurrences by Payment Method



Among the 18 percent of fleet managers who reported fraud or misuse, 73 percent used a credit card, 23 percent had a station account, nine percent used cash, seven percent used driver reimbursement, three percent used either prepaid cards or vouchers and one percent used radio frequency identification (or RFID).

The Tip of the Iceberg

Are card payment methods more prone to fraud, or are they just better at detecting it?

At first glance, it appears that card payment is most susceptible to fraudulent activity. However, the research begs the question: *How much fraud or misuse is going on undetected?* There are virtually no controls over driver reimbursement or the use of cash. In fact, Havill research found a significant drop in the use of cash for fuel purchases. The lack of safeguards is one factor driving this trend. Paper accounts are also subject to abuse because there are no assurances that the transactions logged were actually fuel purchases for a company vehicle.

Blatant fraud, however, is not the only way employees can cost a company extra money. Sometimes, employees may make an honest mistake, such as selecting the wrong fuel grade. With the recent rise in fuel prices, there can be as much as 20 cents per gallon difference between supreme and regular unleaded fuel. This little mistake alone can add 10 percent to the cost of a fill-up.

Risk Management: Select the Right Card Type

How can company officers be assured that their fleet fueling operations are being professionally managed?

Most fleet administrators will find that a card program is required to provide transaction level accountability for fuel purchases. There are three basic card types: fuel only, fuel and maintenance, and purchasing cards. Risk management begins by selecting the appropriate card type.

Fuel only cards restrict drivers to fuel purchases, eliminating the risk of drivers purchasing unauthorized, non-fuel items. When drivers are not responsible for vehicle maintenance and do not need the flexibility to make non-fuel purchases, a fuel only card may be the solution.

Fuel and maintenance cards allow drivers to only purchase fuel and maintenance with the card. This card, again, eliminates the risk of drivers purchasing unauthorized, non-fuel items.

Purchasing cards provide limited restrictions. Some purchasing cards can be configured to restrict purchases to particular merchant types, such as service stations, maintenance providers, hotels, or rental car companies. However, purchases at that merchant are not typically restricted. These cards are appropriate for company executives and sales representatives.

Issuing Cards with Purchase Restrictions

Setting purchase controls at the card level provide drivers the flexibility they need, while at the same time minimizing risk exposure to the firm.

Cards can be issued to the driver or the vehicle. When cards are issued to vehicles, the driver is frequently required to enter a PIN and odometer reading so that the purchase can be linked to the driver. Fleet management reports from the card provider show the fuel consumption in miles per gallon (MPG) for each vehicle. Exception flags are triggered when MPG fall outside of the expected range.

Exception flags can be setup to show purchases outside of normal operating hours as well as weekend transactions. Other exception flags identify unauthorized fuel types, fuel grades, or fueling locations. PIN numbers link driver information to these exception flags.

Lockouts go one step further by restricting these transactions altogether. Unfortunately, many fleet managers cannot take advantage of these added security features because of the diverse needs of their fleet and the inability of their card program to provide these controls at the card level.

Reporting: Key to Detection and Intervention

You can't manage what you can't measure. For this reason, fleet card reporting is the cornerstone of a well managed fleet fueling operation.

A well designed fleet fueling program will not completely eliminate the possibility of fraud and misuse. Purchase restrictions must be 'loose enough' so that card users are not overly inconvenienced as they carry out their duties.

This being the case, a card program is only as good as its reporting system for detecting fraudulent activity. A well designed program puts exception reporting in the forefront so that fleet administrators are quickly alerted to potential problems.

Underneath exception reports, transaction level detail is required so that the fleet administrator can drill down to department level and operator level data, such as:

- Transaction date, time, place, driver or vehicle
- Fuel type, grade, gallons and cost
- Miles Per Gallon

These reports identify vehicles that may need maintenance performed, or may be operated by drivers making personal fuel purchases and charging them to the company's card. A robust reporting system is also useful for scheduling maintenance and identifying problems that may be impacting the efficiency of the fleet.

And of course, when suspicious card activity is detected, the fleet administrator must act quickly. This requires an instantaneous card lockout feature to disable cards that are being misused.

Many Card Programs Lack Security Features

It is a management function to protect the firm's resources from fraud and misuse.

Research published in the 2005 Commercial Fleet Market Study shows that over one-third of fleets are not getting a full array of security features from their card provider. Furthermore, many of the security features that are available are not being used, even though fleets are paying for them through their card fees. According to the study, about half of the fleets using a card program pay a transaction fee, while another third pay a fixed monthly fee.

The bottom line is that fraud and misuse plague the commercial fleet market, as they do vehicle fueling at large. Each fleet and even individuals within the fleet have different needs for purchasing fuel, maintenance, and other business necessities. Fleets following best industry practices have programs in place to minimize their risk. And when abuse does occur, their reporting systems detect it so management can take corrective actions.

Fraud Identification and Prevention Checklist:

- Are you taking advantage of the security features available in the market today? For example, does your payment method restrict or lockout unauthorized purchases so they don't have a chance to occur in the first place, like fuel only cards or time-of-day and day-of-week lockouts?
- Do you have a reporting system that will detect fraud and misuse if it does occur? Are you monitoring fuel consumption on your vehicles and taking advantage of exception reports?
- Is your system flexible so that you can grant privileges to card holders based on their purchasing needs?
- Is your payment solution provider a partner who will sit down with you and design a program based on your needs and the travel patterns of your fleet? What is their track record for preventing fraud and misuse?