VOYAGER®

Fraud, misuse and the bottom line:

Why fleet managers must embrace technology to protect their fleet spend

For fleet managers, fleet card fraud and employee misuse aren't just minor inconveniences – they're ticking financial time bombs that drain company resources and impact the bottom line. Fleet managers report **losing up to 22%** of their fleet spending on fraud and misuse. Depending on the fleet size, these losses can cost their companies hundreds of thousand of dollars, and in some cases, even upwards of millions of dollars annually.

Moreover, while **44% of fleet managers** know these activities impact their business, they don't know how to prevent them. But new technology is emerging to help your company combat fraud and misuse, and you may find some fleet efficiencies and fleet card savings along the way. As fleet managers focus on reducing financial losses and inefficiencies, here are some actionable strategies for reducing the risk of fraud and misuse.

This white paper covers:

- The most significant threats to your fleet card program
- The essential differences between fleet card fraud and misuse
- Eight strategies for reducing your fraud and misuse risk
- How the Voyager solution can enhance your fleet management

What keeps fleet managers up at night?

27%

say fraud and misuse were their most significant challenges over the past year

42%

expect fraud and misuse to be an issue in the coming year

Source: **CFO.com**

The risks to your fleet card program

Before you can attempt to tamp down on fraud and misuse, it's critical to understand each issue for what it is – and what it's not. Let's start with fraud, which refers to the external, illegal use of a fleet card by a third party who is not a company employee. For example, fleet card fraud may entail a criminal using a stolen fleet card for their own purposes. But while fleet cards often require a PIN that only an employee of your company knows, many criminal organizations can illegally obtain card numbers via a card skimmer at a gas pump or store. **Point-of-sale skimming** rose by 16% in 2025, and fraudsters targeted retail outlets and gas stations. **Cloned card fraud** also increased by 24%. These trends show a shift towards high-tech skimming methods.

Employee misuse is different from fraud – and far more common. In these cases, employees use a company-provided card to pay for non-business-related personal purchases. **One survey shows that 62% of corporate employees** are aware of company credit cards being used for non-business-related expenses. In the realm of fleet cards, that may look like filling up the gas tank of a personal vehicle or using the card to buy gas or items at a convenience store for family members. Misuse typically isn't considered fraud because the employee has access to the company card, but it does cost companies. They end up with additional expenses unrelated to their operations and likely not in the budget.

Understanding fraud versus misuse

	FRAUD	MISUSE
Who	Criminals/third parties who are external to the company	Internal employees who have been issued a fleet card
What	They steal or illegally obtain card information to make purchases	They use their employer-provided card for personal purchases and gain
Why	The intent is malicious; fraud is criminal	The intent may be purposeful or a misunderstanding of company policy

The evolving fraud landscape

As fraudsters employ new technology and strategies to improve their success, the fraud landscape is constantly changing. As mentioned, card skimmers are currently one of the most common forms of fraud. However, the bad actors behind these criminal activities are always finding new and better ways to steal information – and they often leverage technology to increase the scale and efficiency of their operations. For instance, some crime organizations now use hidden cameras at gas stations to help capture PIN information as drivers input it. **Other instances** of reported fleet card or fleet-related fraud include:

- **Card not present fraud:** This occurs when criminals use a stolen card number to make purchases, often online. The purchases may be related to transportation or vehicles.
- **Vehicle cloning:** In these cases, fraudsters copy a vehicle's registration number and then use the assigned fleet card to create a duplicate vehicle.
- **Site collusion:** This occurs when a fueling site colludes with drivers to charge more for fuel than they should, and the drivers use the difference to purchase things for themselves. Employees may be involved in this type of fraud, but it goes well beyond misuse.
- **Identity and application fraud:** Like typical identity fraud, criminals apply for cards on behalf of the business and then use the cards for their own purposes.

Fraud trends to watch

- **Card skimming**
- **Stolen PIN numbers**
- **Card not present fraud**
- **Vehicle cloning**
- **Identity and application fraud**

The challenge of employee misuse

As noted, fraud is perpetuated by criminals outside of the company. However, card misuse and abuse are internal problems that stem from how employees use the fleet cards assigned to them. The misuse is often straightforward and may not register as a significant issue to employees in terms of individual transaction amounts.

For example, using an employee fleet card to top off a personal vehicle or make a few purchases at the gas station may equate to a few extra dollars. However, these incidents add up and can cost companies significantly over time. This is especially true if fleet card misuse is widespread among employees across a fleet of several hundred or even thousands of vehicles.

Identifying employee misuse can be difficult. The incidents may occur in conjunction with legitimate expenses or be individual amounts that don't register an in-depth examination. On the other hand, asking employees to clear every expense introduces extra work and may prevent them from completing their jobs. This is where innovative technology like telematics can make a difference.

Telematics uses sensors and other location devices in vehicles to provide companies with insights into driver behavior and vehicle performance. For example, telematics can use this data to help ensure that an employee is using the company fleet card to fill up a company vehicle, flag unusual activity or driver behavior that's impacting fuel efficiency. The technology can help spot misuse and offer insights that improve vehicle and driver performance.

What is telematics?

- Telematics is a technology that collects data from vehicles using GPS and sensors
- Provides insights into driver behavior and vehicle performance, including fuel efficiency
- Can be used to both improve fleet management and combat fraud and misuse

How to reduce fleet card fraud and misuse

Consider the following eight ways to prevent fleet card fraud and misuse:

1. Deactivate cards when not being used and report unauthorized use immediately.

It's not uncommon for organizations to put an unused fleet card in a drawer or envelope and then forget about it. However, anyone can grab an activated card and use it for themselves. To limit this risk, deactivate cards when employees turn them in and report any suspicious use immediately.

2. Implement transaction controls.

Simple spending controls can ensure that employees use fleet cards for their intended purpose. With best-in-class fleet management and fleet card platforms, you can define and maintain spending limits on active cards, drivers, accounts, and vehicles. Many organizations also implement a geographic boundary, meaning the fleet cards only work within a particular state or zip code. That way, if a card number gets stolen, a bad actor can't use it in another part of the country.

3. Leverage telematics to spot unusual behavior and trends.

Integrating telematics data with fleet cards and fleet management platforms allows organizations to track fuel consumption and driver behavior at the individual vehicle level and across your entire fleet. For example, look for platforms with reporting tools and data that make it possible to identify abnormalities quicker, such as a vehicle using far more fuel than the average.

4. Review transaction reports monthly and between billing cycles.

Accessing real-time data enables fleet managers to review spending as it happens. You can leverage APIs to feed the data directly into your system of record. Of course, you gain the ability to spot overspending or potential fraud before it becomes a more significant issue. However, the spending data also enables you to take proactive measures to minimize risk and maximize fleet performance.

5. Keep driver records current.

In addition to knowing who is driving your vehicles, you also want to keep updated information about your employees' driving history. This includes data about license status, traffic violations, medical restrictions, accidents, etc. Maintaining driver records allows you to determine potential risks and make informed decisions regarding the safety of your drivers.

6. Educate employees about misuse and fraud prevention.

Education is a simple but wildly effective way to reduce misuse and motivate your employees to watch for fraud. In many cases, employees may not understand the parameters of misuse – training and reminders can help ensure they're using fleet cards and vehicles as intended. Calling out the consequences of misuse and fraud can deter employees who may be tempted to tap into the company fleet card for personal purposes.

7. Follow up on fraud claims quickly.

First and foremost, you want to stop any ongoing fraud and recover lost funds if possible. However, promptly following up on fraud claims also ensures you spot trends or patterns before they become too widespread or cause significant damage. Your fleet card provider should have 24/7 support to immediately report claims and provide dedicated fraud analysts who can provide limit recommendations and applications.

8. Find a reliable fleet program provider.

A strong relationship with your fleet management vendor is essential, providing connections and experts you can turn to for support and guidance. Connecting with a solution backed by a bank provides added value, including high levels of cybersecurity, reliable uptime, and access to additional banking and credit expertise to help optimize your expense management.

The Voyager Fleet Program difference

With the Voyager fleet management platform and mobile app, your organization can take charge of its fleet card spend – and put that data to work for good. The Voyager Fleet Program offers:

- Fleet-specific credit cards that enable your drivers to purchase fuel, pay for repairs, and even tolls.
- Access to the Voyager fuel station network, which provides negotiated fuel discounts for your drivers.
- A single platform that integrates fuel and vehicle maintenance management, making it easier to manage costs and spot potential issues.
- Additional reporting tools that provide a deep dive into your fleet and fuel-related data reveal areas of potential efficiencies as well as fraud and misuse.
- Mobile applications that route drivers to the lowest-cost fuel centers and enable fueling at pre-determined stations.
- Card restrictions that lock and unlock fleet cards so that employees can only use them for fueling vehicles.
- AI-powered fraud detection that monitors activity and alerts you to high-risk transactions that mirror fraud trends or threats.

Fleet card fraud and misuse are an ever-present threat. Fortunately, technology can help mitigate the risk and optimize fleet operations for improved performance. We turn transparency, risk discipline and focused insight into working solutions you can put on the road. Learn more about what the Voyager Program can do for fleet managers.

VOYAGER®