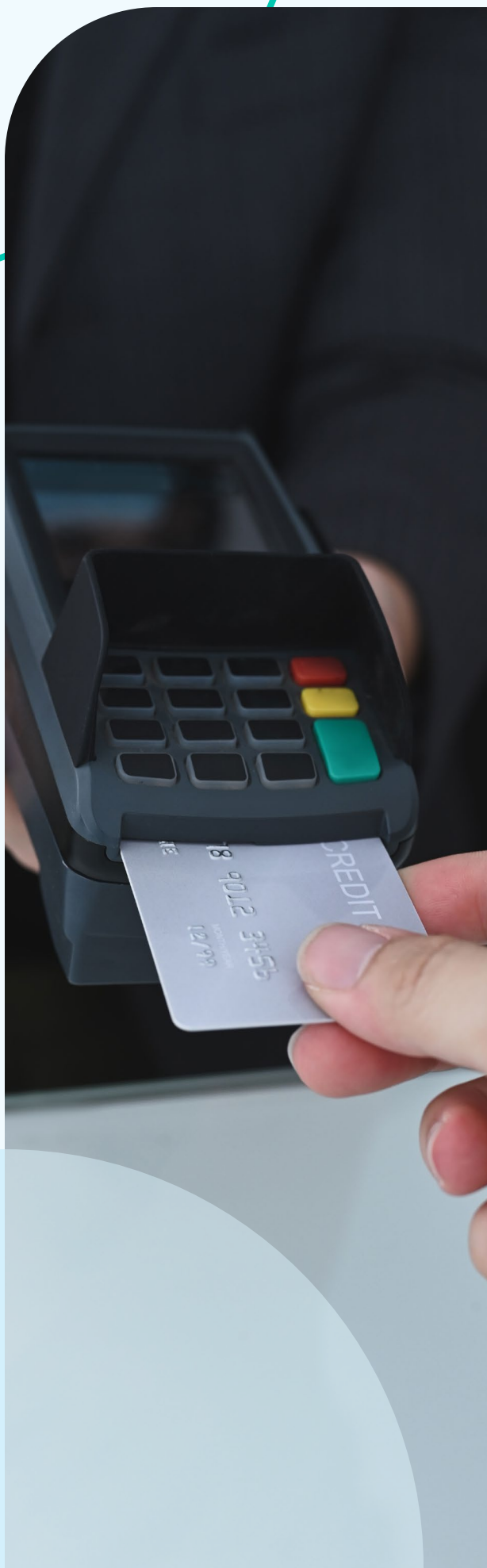


Fuel card fraud:

Understanding the types of fraud and how to protect your business

wex™

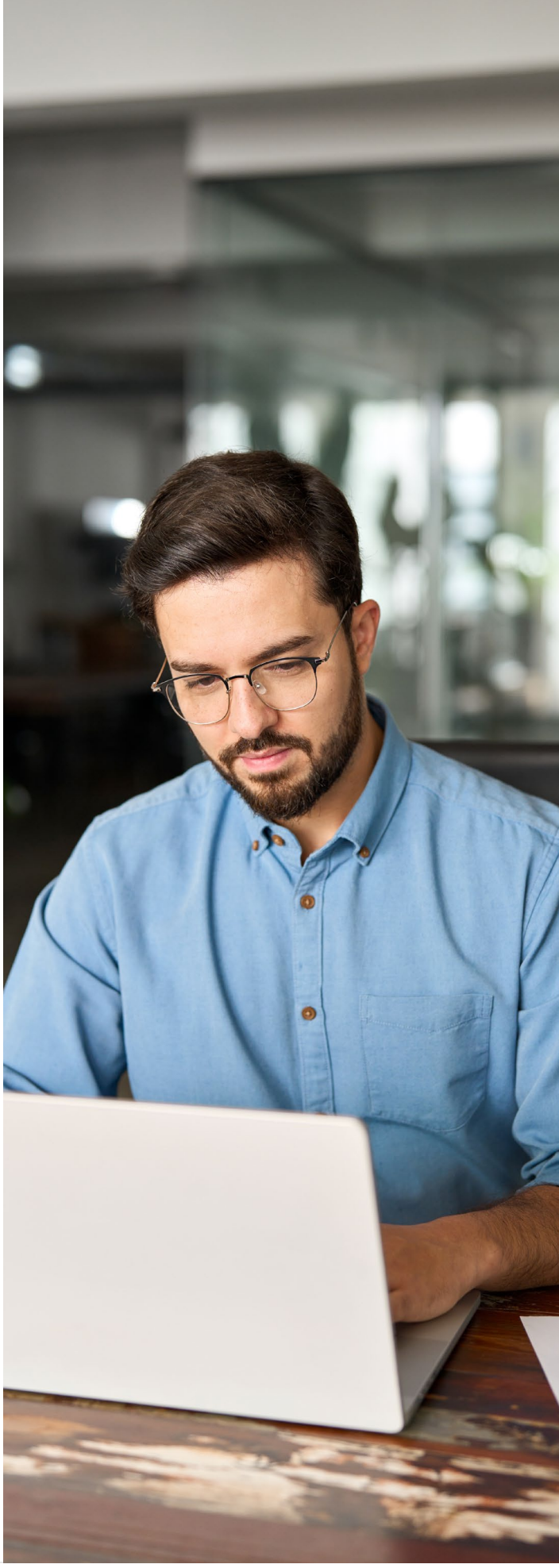
Workfront#_date.2022

Executive summary

In the world of fleet management, fraud is often an invisible expense until the costs start adding up. Whether you're managing a few vehicles or a nationwide operation, your fleet card program can be both a powerful tool for efficiency and a potential target for fraud.

Fraud comes in many forms, but it's not always committed by faceless cybercriminals. In fact, much of it originates from within. This guide breaks down the two major types of fraud that every fleet operator should know: third-party fraud and first-party fraud.

Understanding these risks is the first step toward building a stronger, more resilient fleet operation. With the right mix of policy, data visibility, and fraud controls, fleet managers can spot fraud earlier, prevent losses, and maintain tighter control over their fuel budgets.



1987046955 (6/2025)

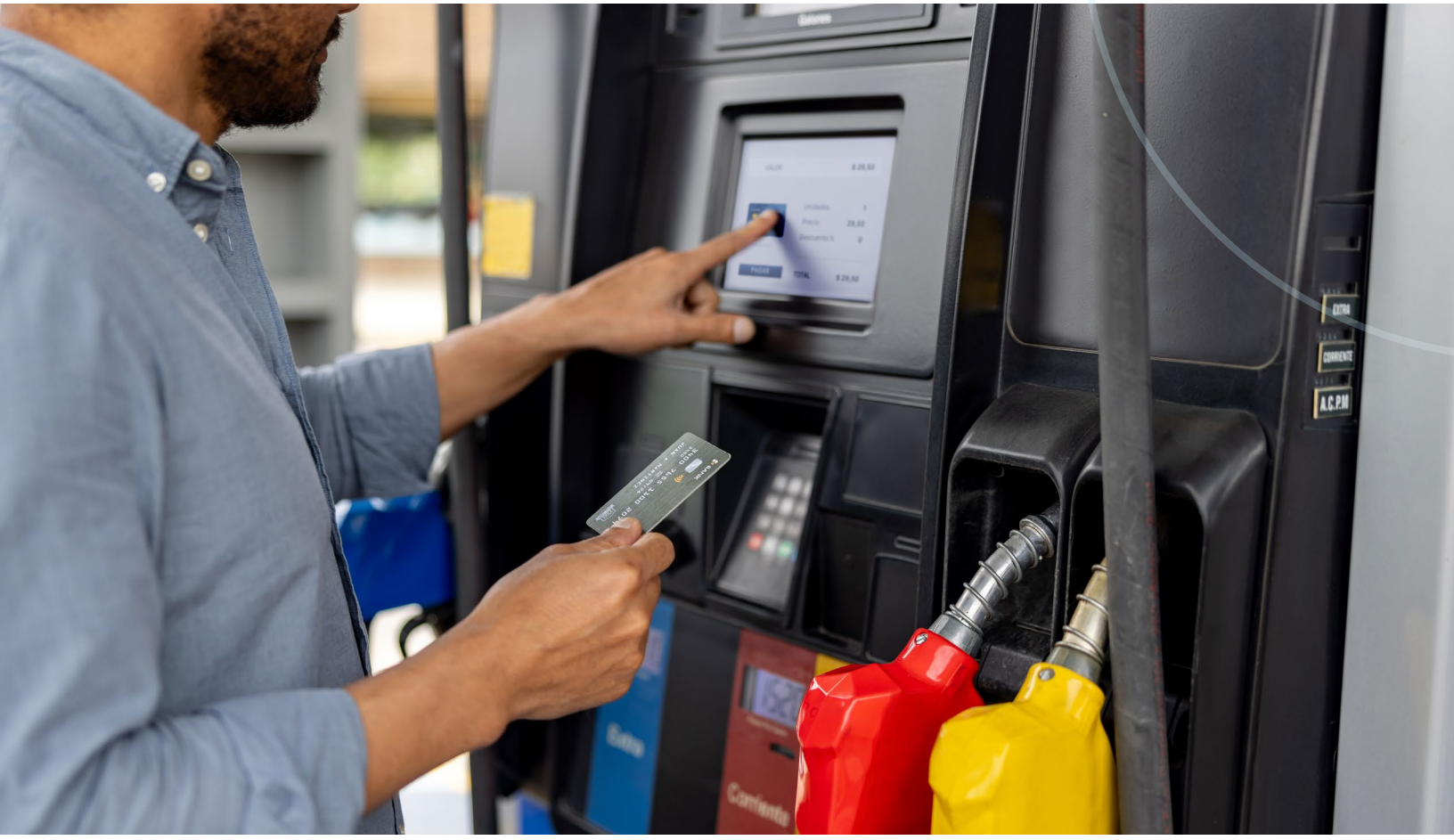
Section 1:

The growing challenge of fleet fraud

Fleet card programs are designed to make managing fuel and maintenance spend easier, but they also introduce new risks if left unchecked. Fraud in the fleet world isn't always headline-grabbing cybercrime; often, it's subtle, hard to spot, and slowly eats away at your bottom line.

From unauthorized fuel purchases to sophisticated skimming schemes, fraud can hit any fleet, large or small. Fleets that rely on outdated tracking methods, loose policy enforcement, or limited transaction oversight are particularly vulnerable.

As more fleets adopt digital tools and remote management practices, fraudsters are adapting, too. And while many businesses focus on external cyber threats, internal misuse can be just as costly, if not more so. That's why understanding the full scope of fraud, from third-party attacks to first-party misuse, is a critical first step in protecting your fleet.



1987046955 (6/2025)

Section 2:

Breaking down the two major types of fleet card fraud

Fleet card fraud isn't one-size-fits-all. To effectively mitigate it, the first step is understanding where the fraud originates and the tactics used to carry it out. Most fraud falls into two broad categories: **third-party fraud** and **first-party fraud**.

Third-party fraud: When outsiders gain unauthorized access

Third-party fraud involves individuals outside your organization, criminals with no legitimate connection to your fleet or business, who obtain and use card information without permission. This type of fraud is often driven by theft, hacking, card cloning, or skimming, and can happen without any direct interaction between the fraudster and your team.

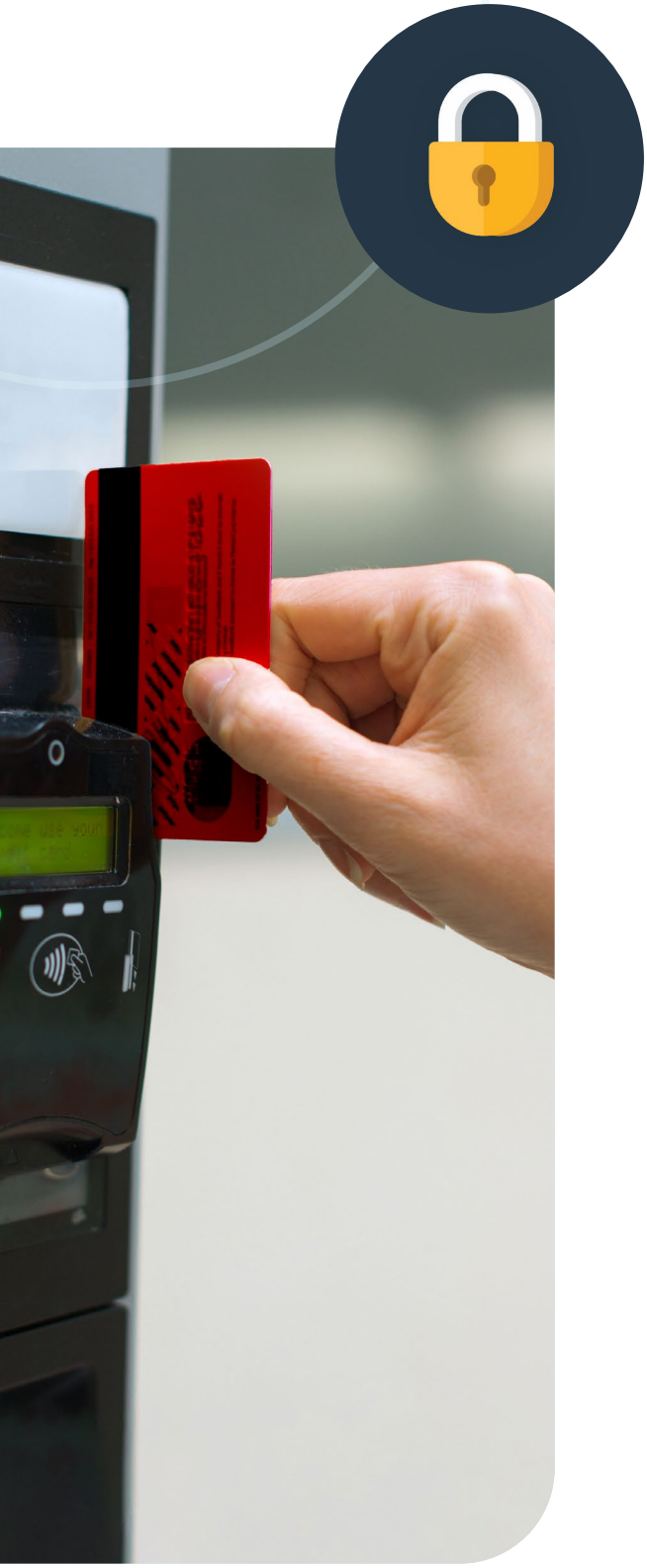
Common examples include:

- **Card skimming at fuel stations:** Devices hidden at the pump capture card data and PINs, which are then used to create counterfeit cards or sell the data to criminals for illegal use.
- **Stolen or lost physical cards:** If a fuel card goes missing and isn't immediately deactivated, it can be used for unauthorized purchases.
- **Data breaches or phishing:** Fraudsters trick employees into revealing account details or obtain data through larger cyberattacks targeting business systems.
- **Account takeover:** A fraudster uses stolen login credentials or social engineering to hijack a legitimate fleet account, changing details, adding cards, or rerouting funds without the business's knowledge.
- **Application fraud:** Criminals submit false or stolen business identities to open fleet card accounts with the intent of running up purchases and abandoning the account once the fraud is detected.

Why it's a challenge:

Third-party fraud is often difficult to spot until significant damage is done, especially if monitoring relies on manual reviews or delayed reporting.

1987046955 (6/2025)



First-party fraud: When the problem comes from within

First-party fraud happens internally, involving someone with legitimate access to the card or account. Typically, this means an employee or driver misusing the card for personal gain or in ways that violate company policy. Unlike third-party fraud, these transactions often take place at approved locations using authorized cards, making them appear routine at first glance.

Common examples include:

- **Personal fill-ups:** A driver uses the company fleet card to fuel their own vehicle or another non-fleet vehicle.
- **Fuel diversion**: A driver fills portable gas containers for resale or personal use in addition to or rather than fueling the fleet vehicle.
- **Excessive transactions:** Multiple back-to-back purchases that exceed the expected fuel capacity or fill frequency of the assigned vehicle.
- **In-store non-fuel purchases:** This type of misuse can be harder to detect when drivers pay for fuel inside the station rather than at the pump, as some merchants may lump fuel and non-fuel items into a single transaction total, making it difficult for fleet managers to spot unapproved purchases without itemized transaction details.
- **Purchasing premium fuel without authorization:** Filling up with higher-grade or premium fuel when your policy specifies regular unleaded, leading to inflated costs.

Why it's a challenge:

First-party fraud can sometimes trigger automated alerts, especially when purchases exceed expected volumes, happen outside of typical patterns, or involve product codes that don't match company policy. But because these transactions often occur at approved merchants and may fall just inside policy thresholds, they can slip through undetected without strong controls. Even when flagged, proving intent and holding individuals accountable can be difficult, especially if the behavior is disguised as a misunderstanding or minor policy violation.

1987046955 (6/2025)

Section 3:

Key warning signs and red flags

The sooner fraud is spotted, the easier it is to stop losses and help prevent future incidents. Whether it's first-party misuse or third-party criminal activity, fraud often leaves behind subtle patterns if you know what to look for. Below are some of the most common red flags that fleet managers and administrators should monitor.

Account alerts

- **Unexpected card reactivation attempts** or repeated PIN entry failures, which can signal card sharing, stolen credentials, or account takeover.
- **New cards or accounts with immediate high-usage,** which are often a sign of fraudulent applications or internal misuse right from the start.

Location irregularities

- **Unusual geographic purchases** occurring outside a driver's assigned route or operational area.
- **Same-day fuel purchases in distant locations** indicating impossible mileage gaps between consecutive transactions.

Merchant behavior

- **Unusual spend patterns at a single merchant** with repeated high-value or high-frequency transactions at the same station.
- **Blended transactions** where fuel and in-store items are combined in one payment (especially if Level III data isn't available to break it down).

Transaction patterns that don't add up

- **Multiple transactions in short timeframes**, especially back-to-back fuel purchases at the same station.
- **Fuel volume exceeding tank capacity** with purchases that don't match the vehicle's make or model specs.
- **Frequent off-hours purchases** made outside of expected business hours or driver schedules.

Driver behavior

- **Purchases at odd times or locations** that don't align with the vehicle's known activity or expected fueling patterns.
- **Premium fuel or add-ons** purchased when policy allows for regular fuel only.
- **Inconsistent fuel types**, such as purchasing diesel for a gasoline vehicle or vice versa, can indicate unauthorized fueling or fuel theft.
- **Fueling multiple vehicles on a single card**, especially when drivers are only assigned one vehicle.
- **Inconsistent odometer reporting** or failure to log mileage accurately, making it harder to track consumption against expected use.

1987046955 (6/2025)

Section 4:

Tools and strategies to strengthen your fraud defenses

While no system can eliminate fraud entirely, the right mix of proactive controls and smart policies can reduce risk and help you stay ahead of suspicious activity. Here are some proven strategies that fleets can use to strengthen their defenses against both first and third-party fraud.

Set clear policies and enforce them consistently

Define what is considered acceptable use, including approved fuel types, spend categories, spending limits, and purchasing hours. Make sure drivers understand the expectations and the consequences for violations.

Use purchase controls to limit exposure

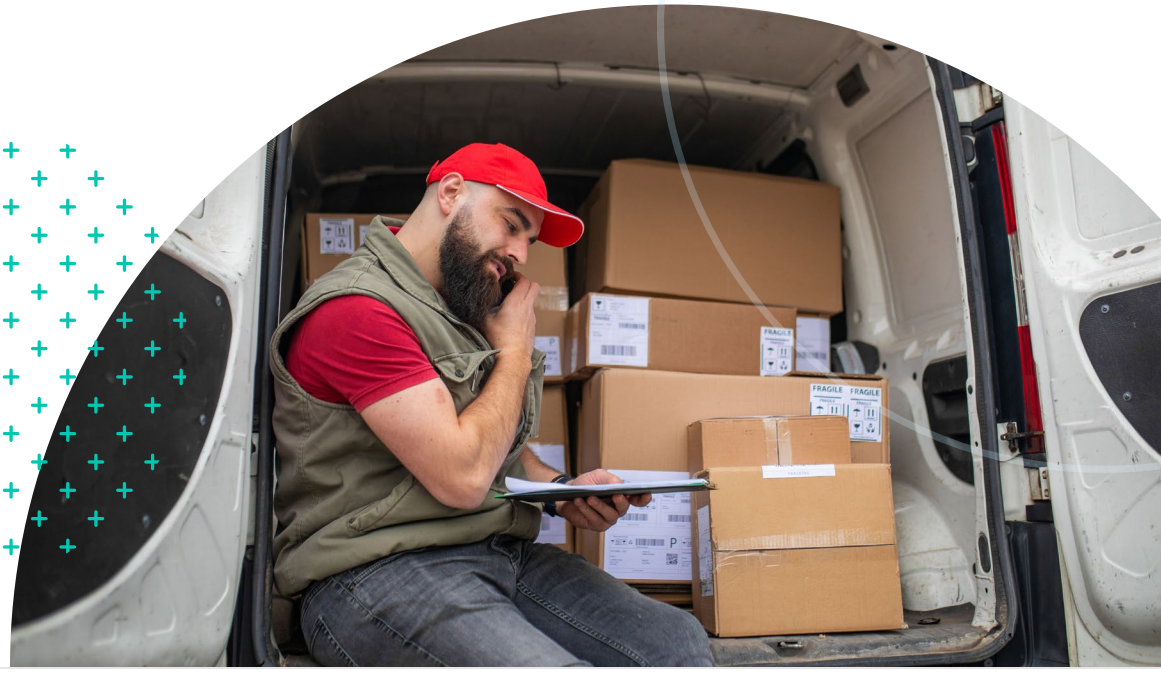
Apply limits on transaction amounts, daily or weekly purchase frequency, and product categories. Adjust these controls to fit the specific needs of each driver or vehicle for better accuracy and security.

Monitor transaction data regularly

Look beyond basic totals and review patterns over time. Pay close attention to volume, frequency, time of day, and geographic trends to spot outliers early. Specifically, review transactions for repeat fueling at the same merchant, especially when those transactions involve unusually large volumes. This pattern could indicate a driver arrangement with the merchant, such as fuel theft or unauthorized reselling.

Leverage real-time alerts and reporting tools

Set up automatic alerts to flag purchases that fall outside of your policy controls, like transactions that exceed limits or don't match assigned driver or vehicle profiles. Alerts for suspicious activity can also help you catch potential fraud early and take action before losses add up.



1987046955 (6/2025)

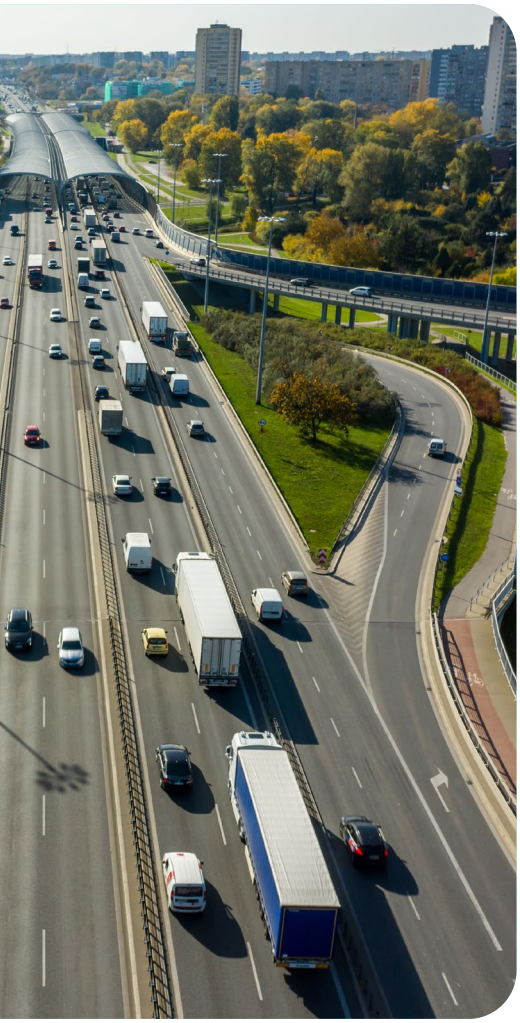
In addition to alerts, regularly reviewing transaction reports can help you spot unusual patterns over time, track driver behavior, and verify that policy rules are being followed across your fleet.

Educate drivers on fraud risks and accountability

Drivers are often the first line of defense. Encourage them to report lost or stolen cards immediately, stay alert for skimming devices, and follow company fueling policies closely.

Secure physical cards and account credentials

Remind drivers to treat fleet cards like cash. Use PINs, set card-level permissions, and deactivate cards quickly when vehicles or drivers leave the company. Emphasize that drivers should never share their unique PINs assigned to the card, as this compromises security and increases the risk of unauthorized use.



Partner with merchants and card providers

Work with trusted fuel networks and card issuers who offer fraud detection tools, transaction data visibility, and account monitoring features designed specifically for fleets.

Take advantage of closed-loop card systems

Unlike general-purpose credit or debit cards, closed-loop fleet cards operate within a controlled network that offers more visibility and tighter enforcement of spending rules. This helps ensure transactions stay within trusted merchants and makes it easier to detect unusual activity. This closed-loop control is what allows for granular, card-level controls that significantly enhance fraud protection. For example, you can implement category-level restrictions (e.g., fuel only, oil and fluids, towing) or limitations on the specific days or times of the week when fueling is permitted.

Leverage enriched transaction data (Level III data)

Fleet cards often capture detailed purchase data, including vehicle ID, odometer readings, and driver prompts, giving you valuable context behind every transaction. In addition, Level III data provides line-item details such as product descriptions, quantities, unit prices, and tax information. This added layer of information makes it easier to control spend, spot outliers, verify spending against policy, and flag potentially fraudulent behavior.

1987046955 (6/2025)

Section 5:

Building a culture of fraud awareness

Fraud prevention is not just about setting controls; it's also about fostering a culture where fraud awareness is part of the everyday mindset. When everyone from drivers to fleet managers understands the importance of fraud prevention, it becomes easier to spot and prevent potential fraud before it escalates.

1. Provide ongoing education and training

Fraud tactics evolve over time, so it's important to regularly educate your fleet drivers and staff on the latest trends and risks. Host training sessions, share educational materials, and keep the conversation about fraud prevention open. The more informed your team is, the better they can detect and respond to potential fraud.

2. Make fraud awareness part of onboarding

When new drivers or fleet employees join, include fraud prevention as a key topic during onboarding. Ensure they understand your company's policies, how to recognize fraudulent activity, and the importance of reporting anything suspicious.

3. Encourage open communication and reporting

Foster an environment where drivers and employees feel comfortable reporting suspicious activity without fear of retaliation. Make sure they know how to report incidents and emphasize that preventing fraud is a team effort.

4. Lead by example

Leadership should set the tone when it comes to fraud awareness. Fleet managers should model best practices, enforce policies consistently, and show that fraud prevention is a priority at every level of the organization.

5. Reward vigilance

Incentivize drivers and staff who actively engage in fraud prevention by rewarding good practices, such as reporting a suspicious transaction or consistently following fuel policies. Recognition can go a long way in reinforcing the importance of vigilance.

1987046955 (6/2025)

Conclusion:

Understanding the differences between **third-party fraud** and **first-party fraud** empowers businesses to build smarter defenses. While no system can eliminate fraud risk entirely, combining the right tools, controls, and policies significantly reduces both exposure and financial loss.

Smarter fraud protection starts with WEX

Preventing fraud isn't just about catching bad actors, it's about setting up the right systems from the start. A fleet card program that gives you visibility, control, and built-in fraud protection tools is one of the most effective ways to stay ahead of both internal and external threats.

That's why choosing the right fleet card provider matters. With WEX, you get:

- **Built-in fraud controls and optional purchase controls** that help catch suspicious transactions before they turn into losses
- **Detailed, line-item transaction data where available (Level III)**, that shows exactly what was purchased, by whom, and where
- **Real-time alerts and customizable reporting** that keep you informed and in control
- **A closed-loop fuel network** designed to limit exposure and help you manage risk more effectively
- **Support and guidance** from a team that knows what fleet managers are up against

If you're serious about reducing fraud and increasing confidence in your fuel spend, the right partner can make all the difference. Smart fraud protection doesn't wait for a red flag. It uses data to predict and prevent issues, keeping your business moving and your spend under control.

Next steps:

Upgrade to a WEX fuel card today for smarter, stronger fraud protection and greater control over your fleet's expenses. https://www.wexinc.com/get-started/

Choosing the right fleet card matters

Look for programs offering:

- Closed-loop security and transaction oversight
- Level III data for deeper insights
- Embedded fraud monitoring and real-time alerts
- Easy-to-configure spending controls

1987046955 (6/2025)