Fortify your fleet:

The case for fraud prevention, fuel controls, and a closed-loop payment system

Executive summary

Fuel card fraud is no longer a rare occurrence—it's an operational threat that every fleet manager must prepare for. In today's complex risk environment, bad actors are becoming more sophisticated, leveraging phishing, card skimming, and even AI-generated scams to exploit weaknesses in fleet payment systems.

The cost of fuel makes up **25%-30%** of the cost of operating a vehicle, and fuel fraud costs businesses a substantial loss of dollars each year. According to a recent **Forbes** article by Virginia Velivela, "the economic losses for commercial driving companies are high—a record 5%-10% of a fleet's annual fuel consumption is lost to theft or misallocation." The true cost goes beyond lost dollars—it includes operational disruption, reputational damage, and time-consuming investigations. Even internal misuse, often undetected, can quietly drain budgets and erode trust.

This white paper explores how fleet managers can **proactively fortify their operations** against fraud by focusing on three critical pillars:

1. **Fraud prevention best practices** to protect against external and internal threats
2. **Purchase controls** that limit what, when, and where fuel cards can be used
3. **Closed-loop payment systems** that provide enhanced visibility, fewer points of failure, and real-time control

As a leader in fleet payment innovation, **WEX offers a proprietary closed-loop network designed specifically to secure fleet fueling transactions**. Unlike traditional open-loop cards, WEX fuel cards offer real-time visibility, Level III data, and robust purchase controls that help prevent fraud before it happens—not after the damage is done.

If your fleet depends on commercial fueling to keep business moving, then securing that spend should be a top priority. This guide will show you how to take the right steps now—before fraud finds your fleet.

Introduction:

Why fraud is a growing threat to fleets

Fuel card fraud is escalating—both in frequency and sophistication. What once might have been a careless driver fueling a personal vehicle on the company dime has evolved into a multi-faceted threat that includes AI-generated phishing emails, cloned cards, skimming devices at fuel pumps, and even insider schemes. Fraudsters are getting smarter, and so must your defenses.

Today's fraud landscape is more advanced than ever.

Scammers are now using artificial intelligence to craft convincing phishing messages that mimic internal communications, tricking employees into sharing card details or login credentials. Meanwhile, skimming devices are being installed discreetly at fuel stations, capturing card data and PINs without detection. And internal misuse—such as unauthorized fueling, card sharing, or purchases of non-fuel items—continues to be an underreported yet costly problem for many fleet-based businesses.

Fleet operations are especially vulnerable.

With dozens or even hundreds of drivers using fuel cards on the road every day, enforcing consistent security protocols becomes a challenge. Decentralized fueling, multiple vendors, and varied driver behaviors create blind spots that fraudsters can exploit. When fuel cards are used without proper controls or oversight, the risk of misuse increases dramatically.

The cost of inaction is high.

Beyond direct financial loss, fraud can result in operational disruption, delays in reconciliation, audits, and a loss of trust across teams. Reputational harm—especially for businesses that serve high-profile clients or operate government contracts—can be difficult to repair. For small and mid-sized fleets in particular, a single fraud incident can have outsized consequences.

Traditional credit cards aren’t designed for fleet security.

Open-loop credit card systems route transactions through third-party networks with limited visibility and fewer controls. These systems typically lack detailed data capture (such as fuel type or odometer readings), and real-time transaction monitoring. This opens the door to both accidental misuse and deliberate fraud, leaving fleet managers scrambling to detect and respond after the fact.

To stay ahead of evolving threats, fleet managers need purpose-built tools that offer tight controls, transaction transparency, and a secure network designed specifically for fueling. That’s where WEX—and the power of a closed-loop system—comes in.

Fleet fraud at a glance:
Top 5 vulnerabilities to watch

1. **Card skimming at fuel stations**
   Criminals install hidden devices that capture card data and PINs—often without drivers noticing.
2. **Phishing scams targeting drivers or admins**
   AI-generated emails can trick employees into revealing card numbers or login credentials.
3. **Internal misuse of cards**
   Drivers may purchase unauthorized fuel, fill personal vehicles, or make off-hours transactions undetected.
4. **Lack of purchase controls**
   Without location or spending limits, cards are more susceptible to abuse and fraud.
5. **Using open-loop credit cards**
   Traditional credit cards offer less visibility, slower fraud detection, and fewer ways to lock down spending.

Fuel card fraud—how it happens and how it hurts

Fuel card fraud can take many forms—and it rarely looks the same twice. Whether it's an external cybercriminal intercepting card data or a trusted employee bending the rules, fraud introduces serious financial and operational risk for fleets of all sizes. To effectively defend against these threats, fleet managers need to understand where vulnerabilities exist—and how those breaches can impact their business.

External fraud: Attacks from the outside

External fuel card fraud is often sophisticated and difficult to detect until after the damage is done. These are some of the most common external threats:

- **Card skimming:** Fraudsters install hidden devices on fuel pumps to steal card information and PINs. These devices are small, discreet, and capable of cloning multiple cards in a single day.
- **Phishing scams:** Increasingly advanced emails or texts impersonate internal teams or vendors, luring employees into disclosing sensitive card or login information.
- **Cloned or counterfeit cards:** Once card data is stolen, criminals create duplicates that can be used to make unauthorized purchases before the fraud is flagged.

Internal fraud: Misuse from within the fleet

Not all fraud is high-tech—sometimes it comes from within. Internal misuse of fuel cards is often overlooked but can be just as costly over time.

- **Off-hours fueling:** Drivers may use cards to fill personal vehicles or assist friends/family outside of work hours.
- **Purchasing non-fuel items:** In the absence of fuel-type controls, drivers can use cards for convenience store items, drinks, or even car washes that aren't approved.
- **Card sharing:** A single card passed between multiple drivers or vehicles makes it nearly impossible to track accountability.

Pro tip:

Set up automatic alerts for irregular fuel purchases and regularly audit fuel spend against routes and odometer logs.

Real-world example: What a single incident can cost

A regional construction company with a fleet of 25 vans noticed an unusual uptick in fuel expenses. After reviewing transaction reports, they discovered one driver had been using the company fuel card to fill his personal truck over the course of several months. The purchases fell just below the company's weekly review threshold and went undetected until a fuel audit surfaced the discrepancy.

Total estimated loss: $3,200 over 90 days.

That figure doesn't include time spent on internal investigation, card replacement, or legal action.

The hidden costs of fuel card fraud

The true cost of fraud isn't limited to the dollars stolen at the pump. It ripples through the business in less visible ways:

- **Chargebacks and reimbursement disputes:** Time-consuming and often unresolved in your favor.
- **Reconciliation issues:** Fraudulent or duplicate charges can throw off reporting and delay closeouts.
- **Loss of trust:** In cases of internal misuse, morale and management credibility can suffer.
- **Compliance concerns and audits:** Repeat fraud incidents may prompt regulatory reviews or customer concerns—especially in government or enterprise contracts.

When left unaddressed, fuel card fraud doesn't just drain budgets—it erodes operational confidence. That's why proactive prevention is no longer optional—it's a competitive and financial imperative.

Fraud red flags: What to watch for in your fleet reports

Keep an eye out for these common indicators that fuel card misuse or fraud may be occurring:

Red flag	What it might indicate
Fuel purchases outside of business hours	Off-hours personal use or unauthorized fueling
Same card used for multiple transactions in a short time	Card sharing or skimming attack
Premium or non-approved fuel types	Driver misuse or lack of fuel-type controls
Fueling far from job site or home base	Potential skimming, unauthorized use, or ghost fueling
Fuel volume exceeds tank capacity	Fraudulent transactions or falsified odometer readings
Non-fuel purchases at convenience stores	Purchase of unauthorized items or snacks
Frequent small charges under threshold	Intentional pattern to evade review or limits

The power of fuel controls to prevent fraud

Even the most advanced fraud detection tools can only do so much without preventative measures in place. That's where fuel card controls make a powerful difference. When implemented effectively, these built-in guardrails can stop fraud and misuse before a transaction ever occurs—saving time, money, and administrative hassle.

Smart controls, safer spending

Fuel card controls give fleet managers the ability to set specific rules for when, where, and how a card can be used. These controls help eliminate the gray areas that allow fraud to flourish, while also limiting the impact of honest mistakes.

Here's how each control feature works to reduce fraud:

Non fuel-type restrictions
Eliminate the risk of non-fuel purchases. Cards can be restricted from being used inside the store to purchase snacks, gift cards, or other unapproved items.

Time-of-day and location limits
Limit purchases to business hours or to fueling stations within a specific geographic region. If a card is used outside the approved window—or in an unexpected location—the transaction is declined or flagged.

Gallon and dollar thresholds
Set maximum purchase limits per transaction, per day, or per week. These caps prevent bulk purchasing, unauthorized fill-ups, or subtle overages that often go unnoticed without oversight.

Vehicle or driver ID matching
Require vehicle or driver identification before every transaction. This adds accountability to each card swipe and deters sharing cards between drivers or fueling unauthorized vehicles.

Fuel card controls vs. traditional credit cards

Most credit cards used for fleet fuel purchases operate on open-loop systems, designed for general business expenses—not specialized fleet controls. Here's how they stack up:

Control feature	Fuel card (e.g., WEX)	Traditional credit card
Non-fuel restrictions	✓ Yes	✗ No
Time-of-day purchase limits	✓ Yes	✗ No
Location/geofence control	✓ Yes	✗ No
Gallon/dollar thresholds	✓ Yes	✗ No
Vehicle/driver ID enforcement	✓ Yes	✗ No
Real-time alerts & controls	✓ Yes	✗ Limited
Fleet-specific reporting	✓ Detailed	✗ Basic

The return on prevention

Fuel card controls offer a direct return on investment by reducing unauthorized spend and streamlining administrative oversight. Here's how:

- **Fewer fraudulent transactions:** Proactive controls block misuse before it happens, cutting fraud-related costs.
- **Reduced administrative burden:** Less time spent reconciling transactions, investigating misuse, or issuing chargebacks.
- **Improved driver accountability:** With clear limits and individual identification, drivers are more mindful of fuel behavior.
- **Better budget visibility:** Real-time data helps fleet managers monitor trends, adjust thresholds, and forecast fuel spend with accuracy.

For WEX customers, these controls aren't just optional—they're built into the system and configurable to meet your fleet's specific needs. When combined with a closed-loop payment network, fuel controls serve as a critical first line of defense in your fraud prevention strategy.

Why closed-loop payment systems offer superior protection

Fraud prevention doesn't end at the pump—it continues behind the scenes through the network that powers your transactions. For fleet managers serious about securing every dollar spent on fuel, the type of payment system you use matters.

That's where a **closed-loop payment system** gives your business a distinct advantage over traditional open-loop credit cards.

Closed-loop vs. open-loop: What's the difference?

Open-loop systems (like those used by most credit cards) process transactions through a wide network of third-party banks, issuers, and processors. These systems are designed for broad, general-purpose use, not fleet-specific needs.

Closed-loop systems (like the WEX network) operate on a **proprietary payment platform** where transactions flow directly between the fleet card provider, approved merchants, and the business. This tighter, more controlled environment improves visibility, security, and control.

Fewer intermediaries = fewer points of failure

With open-loop cards, every transaction can pass through multiple parties—each introducing a potential vulnerability. Skimming, delayed fraud detection, inconsistent data formatting, and misclassified purchases are more common in open networks.

In contrast, WEX's **closed-loop network** simplifies the transaction path. Fewer middlemen means:

- Reduced exposure to third-party fraud risks
- Faster transaction approvals
- Better data integrity
- Consistent fraud monitoring based on fleet-specific patterns

Level III transaction data: Visibility that drives action

WEX's closed-loop system captures **Level III data**, giving fleet managers detailed insights beyond the basics of when and where a transaction took place. Each transaction can include:

- Fuel type purchased
- Gallons dispensed
- Price per gallon
- Vehicle and driver ID
- Location and time of transaction
- Odometer reading (if required at time of purchase)

This rich data not only helps spot irregularities—it also supports more accurate fuel forecasting, cost allocation, and reporting.

Faster fraud detection and easier audits

With real-time visibility and consistent transaction formatting, fleet managers can more easily identify suspicious activity and flag anomalies—such as fueling outside approved hours, high-frequency transactions, or purchases inconsistent with vehicle specs.

This improved transparency means:

- Faster internal audits
- Fewer disputes and chargebacks
- More confident compliance with internal policies and external contracts

A system built for fleets—not for general business use

Ultimately, a closed-loop system isn't just more secure—it's more **fleet-aware.**

Every control, data point, and process is purpose-built to support businesses that rely on commercial vehicles. That makes WEX's network not just a payment system—but a fraud defense mechanism that evolves with your needs.

Choosing the right partner to secure your fleet spend

Fraud prevention isn't just about implementing the right tools—it's also about working with a partner who understands the unique risks, pressures, and workflows of fleet operations. As the fuel payment landscape evolves, choosing a provider that offers not only technology, but expertise, can mean the difference between reactive and proactive risk management.

What to look for in a secure fleet card provider

Not all fleet card programs offer the same level of protection. Many rely on a traditional banking infrastructure or open-loop systems that weren't designed for fleet-specific needs. When evaluating providers, prioritize those that combine advanced fraud detection with custom controls, real-time visibility, and a purpose-built network.

Checklist: Fraud-prevention features to demand

Not all fleet card programs offer the same level of protection. Many rely on traditional banking infrastructure or open-loop systems that weren't designed for fleet-specific needs. When evaluating providers, prioritize those that combine advanced fraud detection with custom controls, real-time visibility, and a purpose-built network.

Feature	Why it matters
□ Closed-loop payment network	Reduces fraud risk with fewer intermediaries
□ Customizable purchase controls	Helps prevent unauthorized spending
□ Real-time transaction monitoring	Detects and blocks fraud before it escalates
□ Level III data capture	Provides detailed insights into every transaction
□ Product restrictions	Prevents non-fuel purchases
□ Time-of-day and location limits	Stops off-hours and out-of-route transactions
□ Vehicle and driver ID verification	Adds accountability to every purchase
□ 24/7 fraud support and account management	Ensures fast response to emerging threats

If your current provider can't check all of these boxes, your fleet may be more exposed than you realize.

Customer spotlight:

How one business owner got ahead of fraud

> "I'm able to control and see everything from afar and not have to worry about what my technicians are spending on fuel, where they're fueling, whether they're engaging in a lot of idling. All of these things I can monitor from the WEX app, and manage my team accordingly."

— Manny Muniz, Business Owner
Full Metal Mechanical
Regional HVAC Services Company

WEX: A trusted partner in fleet security

With more than 40 years of experience serving North American fleets, **WEX is a recognized leader in fleet payment security and fraud prevention**. Our closed-loop network is designed from the ground up to support the complexities of fleet fueling—offering real-time visibility, advanced controls, and a dedicated fraud monitoring team.

WEX doesn't just process transactions—we provide the infrastructure and intelligence to help you fuel with confidence. Whether you're managing five vehicles or five thousand, our solutions scale with your needs and are backed by responsive, expert support.

When every transaction counts, you need a partner who treats your fleet spend like their own. WEX delivers the technology, transparency, and trust you need to protect your business at every pump.

Conclusion:

Fortify your fleet before fraud finds you

Fuel card fraud isn't a question of "if"—it's a matter of "when." In today's fast-moving and increasingly complex risk landscape, reactive strategies are no longer enough. To stay ahead, fleet operators must take a proactive stance—tightening controls, securing transaction pathways, and partnering with providers who understand the unique demands of fleet operations.

Throughout this paper, we've explored how WEX helps businesses defend their fuel spend with three key strategies:

- **Proactive fraud prevention**, through built-in monitoring, real-time alerts, and a dedicated support team
- **Airtight purchase controls**, including time-of-day limits, location geofencing, and driver/vehicle ID requirements
- **A secure closed-loop payment network**, designed specifically for fleets, with fewer intermediaries and superior data visibility through Level III transaction detail

Together, these tools help fleet managers reduce fraud exposure, increase operational efficiency, and gain peace of mind.

The **cost of inaction** can be steep—lost revenue, damaged trust, compliance risk, and additional administrative overhead. Even minor, repeated misuse can quietly erode your margins if left unchecked. But the right controls and systems can stop fraud before it starts.

Now is the time to assess your current setup:

- Are you using an open-loop card with limited visibility?
- Do you have the ability to restrict transactions by type of purchase, time, and driver?
- Are fraudulent or questionable transactions going undetected?

If the answer to any of these questions is "no" or "I'm not sure," your fleet could be vulnerable.

WEX is here to help you take control. With decades of experience serving fleets globally, a purpose-built payment network, and unmatched fraud prevention features, WEX is more than a fuel card provider—we're your partner in fleet security.

Protect every gallon, every transaction, every time.

Fortify your fleet before fraud finds you.

Learn more at **wexinc.com**.

You’ve taken the first step by learning how fraud prevention, purchase controls, and a closed-loop payment system can protect your fleet. Now it’s time to put those insights into action.

Download the companion checklist

Download our **Fuel card fraud prevention checklist** to help you assess vulnerabilities, implement smarter controls, and protect your fuel spend.

References:

Shell
Forbes