Leveraging smarter fraud detection for better fleet management

WEX | TRUCKINGDIVE

Custom content for WEX from Studio by Informa TechTarget

Introduction

With an uncertain economy, inflation, and rising fuel costs threatening the bottom line for many companies, fleet managers are under growing pressure to cut costs. This task can be easier said than done for asset-heavy businesses that maintain fleets of service vans, delivery trucks, cars, pick-up trucks, buses or other light- and medium-duty vehicles. Fleets such as these can require constant expenditures on fuel and maintenance to keep operations running smoothly. But another, quieter factor at play in commercial fleets significantly erodes margins as well — fraud.

The elaborate card-skimming rings that have plagued the industry for decades are getting more organized and more sophisticated, while phishing schemes and other external threats are on the rise.

Meanwhile, many fleets face internal risks, such as drivers using company cards for personal purchases or taking cash at the pump to fill up non-company vehicles on the company dime. These malicious activities can add up fast. Industry research shows that 19% to 22% of fleet spend is actively lost to theft and fraud, while up to 10% of annual fuel consumption can be attributed to theft or misallocation.[1]

In the age of artificial intelligence, fraud is not only easier to produce — it's also harder to detect. This playbook will explore how AI-driven fraud protection and telematics integration can help public and commercial fleet operators safeguard operations against bad actors to bring costs under control.

[1] "Fuel card fraud is on the rise: How two-factor authentication and telematics help protect your trucking fleet," WEX Mobility, https://www.wexinc.com/wp-content/uploads/2025/08/Telematics-Dynamic-Prompt-WEX-Whitepaper.pdf

Understanding the modern fraud landscape

Unlike long-haul trucking, where fueling often happens at scheduled stops and purchase amounts remain more predictable, company or public vehicle fleets tend to fuel up more sporadically and make more stops. Dozens or hundreds of company cards might be in use, resulting in hundreds or thousands of charges per month. Sorting through that activity to uncover misuse can be daunting, especially when reviewing transactions manually or using outdated systems.

"Attack velocities are substantially higher than they have been," said William Fitzgerald, vice president of global anti-financial crimes at WEX®, a company simplifying complex markets by connecting businesses, payments, and data. "Fraud attempts in the industry are in some cases two times higher than they were at the beginning of the year. Even if your fraud capture rate is on par or slightly improved, the cost of fraud is still higher because the velocity is higher."

Essentially, fraud risk comes in two forms:
internal and external.

"Fraud attempts in the industry are in some cases two times higher than they were at the beginning of the year."

William Fitzgerald
Vice President of Global Anti-financial Crimes, WEX

External attacks

Fuel card fraud was once primarily a physical activity. Bad actors would memorize card numbers or swipe cards left behind at gas stations. Over time, fraudsters have become more sophisticated, installing card skimmers at the pump. These skimmers record card numbers and PINs, enabling them to clone physical cards for use. This activity has grown to a massive scale, with FBI estimates placing skimming-related losses at $1 billion annually.[2]

Fitzgerald also reiterated that AI has significantly increased the sophistication of scammers' attacks, enabling them to target businesses in new and increasingly more believable ways. "I absolutely would attribute the increased complexity of fraudulent activity to the advent of interface-based AI," he said. "Generative AI tools provide people who want to activate phishing schemes and social engineering tactics a level of speed and complexity to their tactics that's unprecedented. It's really eliminated the barrier to entry for fraud."

› FBI estimates place skimming-related losses **at $1 billion annually.[2]**

"Friendly" fraud

For many fleets, however, the most common form of fraud comes from inside the house. Drivers, whether ignorantly or maliciously, often misuse company cards to buy things they shouldn't.

"On a recent call with several fleet managers from across a range of industries, Internal theft was the number one issue discussed," said Cecile Zinder, vice president – mobility products for WEX. "A fleet with $5 million in annual fuel spend could be losing up to $250,000 to internal and external fraud, with the majority of that coming from internal fraud. That dollar amount does not include the operational and legal costs associated with managing those fraud cases."

Given these numbers, fraud prevention goes beyond a simple security issue and becomes a cost-control issue with a major impact on a fleet's margins, efficiency, and accountability.

[2] "Commond Frauds & Scams: Skimming," Federal Burea of Investigation, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming

Where traditional protections fall short

Many fleets still rely on basic protections such as PIN codes, purchase limits, or manual audits to secure their fuel spending. As fleets grow, however, so does the volume of data that must be monitored and analyzed to identify fraudulent activity. Unfortunately, using solely reactive methods doesn't allow you to keep up with modern risks.

"Many fleet managers use more than 13 tools to operate their business," said Chris Hodge, director of product management at WEX. "They're in a position where they have more data than they've ever had, but many also tell us they feel like they have never had less understanding of what all the data means. There has been a rapid injection of noise, and fleets can't find the signal."

With paper audits and static rules, fleet managers and auditors may only catch the most obvious incidents. Fraudulent activity may go undetected for weeks, if it is even discovered at all. "For a long time, binary rules were the standard," Fitzgerald said. "It was if/then statements, like if a driver travels to a location under a certain amount of time, decline the transaction. You can string a few of those together, but they're still binary."

Hodge likened fraud to electricity — it will go where it's easiest to go. As the technology available to fraudsters increases in sophistication, businesses must evolve along with it. Modern fleets need real-time visibility and predictive controls that evolve as fast as new schemes and cybersecurity threats do.

The role of AI in modern fraud prevention

Thankfully, bad actors aren't the only ones with access to artificial intelligence tools. AI-assisted fleet management tools allow fleet operators to analyze millions of transactions and detect anomalies in mere seconds.

For example, WEX's fraud engine analyzes roughly 30 million transactions each month. This is a material advantage when that data is used to re-train its models every 30 days. That ongoing machine learning activity ensures WEX's payment systems understand and incorporate the latest trends in fraudulent activity. Since deploying its AI models, over a single 60-day period WEX achieved a 32% increase in fraudulent transaction capture and a similar improvement in false-positive accuracy.

"Capturing more fraud often means more false positives," Fitzgerald said. "But our models achieved gains in both precision and recall. That's a big deal for fleets that can't afford downtime."

› Over a single 60-day period WEX achieved a **32% increase in fraudulent transaction capture**

By incorporating AI insights into its well-established SecureFuel solution, WEX applied machine learning to transaction and telematics data. SecureFuel flags unusual fueling behavior in real-time. The incorporation of telematics data also facilitates the use of geodesic rules, such as route patterns, time of day, and bounding boxes, enabling systems to identify deviations from a driver's normal fueling behavior. For example, if a van is fueling miles away from its intended job site, the system alerts a manager or declines the transaction.

"We're integrating telematics software so that fueling decisions can be made based on vehicle proximity, tank capacity, and other data," said Zinder. "It's a powerful tool. Fraud rates among fleets using SecureFuel users over on our OTR side of the business are nearly zero."

The rise of agentic AI is also making it easier for fleet managers to process, analyze, and understand the massive amounts of data they collect from different systems, which might otherwise go unexamined.

"AI makes fleet data more digestible," Zinder added. "Imagine a chatbot that can answer questions like, 'Which drivers spent the most last week?' or 'Are there any anomalies in my accounts?' It's about creating a more intuitive, real-time experience for fleet managers."

In the near future, AI agents will likely take another step forward, gaining the ability to recommend or initiate actions in near real time. "Eventually, we'll likely be able to predict downstream fraud from upstream cyber signals. Everything is interconnected," Fitzgerald said.

What to look for in a fuel fraud detection solution

Providers of fuel cards and fleet management technologies must understand the threats light- and medium-duty vehicle fleet operators face and build fraud protection into the solution to help them mitigate risk.

When evaluating current or potential payment partners, here are some features to look for:

- **Level 3 transaction visibility.** A provider should offer detailed purchase data, such as product type, quantity, and cost, to help fleet managers easily spot misuse.
- **Closed-loop payment network.** This ensures transactions remain within a secure ecosystem, allowing faster fraud detection and fewer false positives.
- **AI-driven anomaly detection at scale.** A partner's AI model should continuously learn from millions of transactions, enabling it to spot even the latest schemes.
- **Telematics integration.** Integrating telematics data into your operations enables fleet managers to detect whether the right vehicle is fueling at the right place and at the right time.
- **Automated alerts and controls.** The system should automatically alert fleet managers and block suspicious purchases instantly.

Lowering fleet costs through **better fraud prevention**

In today's complex fleet management environment, fraud prevention is a critical component of any cost-control effort. Malicious actors have expanded their schemes beyond what traditional protections like PIN codes and manual audits can handle, and fleet managers must engage providers that can help them fight modern fraud with modern solutions.

With smarter technology, real-time visibility and predictive analytics, fleet managers can worry less about fraudulent spend and stay focused on what matters most — keeping vehicles moving, drivers safe, and budgets on track.

To learn more about AI-powered fraud protection in your commercial or public fleet fuel program, contact WEX today.

About us

WEX (NYSE: WEX) is the global commerce platform that simplifies the business of running a business. WEX has created a powerful ecosystem that offers seamlessly embedded, personalized solutions for its customers around the world. Through its rich data and specialized expertise in simplifying benefits, reimagining mobility, and paying and getting paid, WEX aims to make it easy for companies to overcome complexity and reach their full potential.
For more information, please visit wexinc.com.

Studio
by informa techtarget

Expert led.
Impact driven.

Studio is Informa TechTarget's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more