

Fleet fraud protection: AI technology to beat the fraudsters



Introduction

If you're a fleet manager, fraud has likely been a topic in your work in the last several months. According to **TRM Labs**, fraud has been skyrocketing since 2024, and the Federal Trade Commission estimated that in 2025 **the overall cost of fraud to consumers may have been as high as $196 billion**. In this report, we'll cover how this world-wide increase in fraud impacts businesses with commercial vehicle fleets. We'll also cover how artificial intelligence can help fleets beat the fraudsters at their game.

The fraud problem for fleet managers

It's hard to believe just how pervasive fraud has become in a short span of years. In 2023, **29% of adults** experienced account takeover, and 75% of account takeover attacks start with a phishing scheme. Account takeover through phishing and social engineering is the biggest risk in the fraud space today.

Generative AI has made phishing attacks more sophisticated. Since the fourth quarter of 2022 when ChatGPT launched, there's been a **1265% increase** in malicious phishing attacks.

As we face the daunting challenge of pervasive fraud attempts, for fleet managers the question becomes where is fraud impacting my business. We'll explore what experts are reporting and where fleets can shore up protective guardrails.

Two ways fleets are most experiencing fraud

William Fitzgerald, Vice President, Global Fraud & Financial Crimes at WEX, says that while fleets are experiencing fraud at the pump, the place fraud is hitting hardest is through identity theft. "Today, we're seeing the primary fraud attack on fleets happen through application fraud. Business identity theft is on the rise." With the advent of generative AI, access to information allowing fraudsters to obtain credit lines has become relatively easy. "With any AI engine, you can prompt your machine to learn anything you want about a business, collect that information, and then use it to fraudulently obtain credit lines."

> Today, we're seeing the primary fraud attack on fleets happen through application fraud. Business identity theft is on the rise."
>
> **William Fitzgerald**
> *Vice President, Global Fraud & Financial Crimes at WEX*



First-party fraud is also a common concern in businesses with a fleet of commercial vehicles. "Fuel fraud, including unauthorized fuel card use and skimming, can significantly erode the profitability of fleet operations, with fraud rates going as high as 12%," says Fitzgerald.

Anytime an authorized representative makes a transaction using their own identity to commit fraud, it's called first-party fraud. First-party fraud is both the most obvious to detect and at the same time the most difficult to prosecute. This is because the user perpetrating the fraud can easily authenticate the transactions they are making: they are the person authorized to use the credit. Fraud alerts intended to deter illegal purchases are easily bypassed by someone authorized to use a line of credit, which makes catching the criminal activity difficult.

What is the difference between first-party and third-party fraud?

Inside attacks—also known as first-party fraud—come from the people within your company. Outside attacks come from strangers.

First-party fraud

A common misperception in mobility is that "fraud" and "card misuse" are two different things. They're not. "Card misuse" is first-party fraud. It's fraud that's tied to company policy. "If an employee is not complying with the expense policy of the organization in which they work, that is first-party fraud, and that's something that every fleet manager and business owner that has employees is thinking about all day, every day," says Cecile Zinder, Vice President of Product at WEX.

Common examples of first-party fraud 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.

Third-party fraud

Third-party fraud is conducted by a perpetrator outside of your organization. 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 of third-party fraud 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.

> For first-party fraud, the expense of recovering from that would include lost capital, legal fees, the resources and time spent on investigations and training."
>
> **Cecile Zinder**
> *Vice President of Product at WEX*

Regulatory scrutiny and the compliance imperative

As fraudulent activity increases, it is also becoming more sophisticated, harder to detect, and more costly for businesses – **71% of organizations** reported a rise in fraud attacks in 2025.

The largest factor in this shift is AI. Artificial intelligence has removed the barrier to entry for phishing. You don't have to speak the language of the person or company you're defrauding, or understand the economy that you're operating in to commit fraud. You can ask an AI chatbot questions, and the tool will generate an email or a phone call or text message, and not only generate it, but also perform the fraudulent activity for you.

"We're seeing more phone-based phishing schemes where AI is making the phone calls," says Fitzgerald. Before generative AI, if you had an offshore fraud team, this kind of activity was not possible. Now it is. The AI voice is so life-like that criminals can start collecting information over the phone from unwitting customers.

The hidden costs of fraud

Recovering from fraud can be surprisingly expensive: it's not just the dollars lost to the actual fraud that impact a business's bottom line. There are hidden costs with fraud including operational costs associated with preventing internal fraud. The expense of nabbing the perpetrator and shoring up against future fraud are not insignificant. It takes time to monitor drivers for fraudulent behavior, to pore through reports, and to call a driver off the road and interview them. Time and costs accrue, which is not in your best interest. Then, if you determine there was fraud, you may be facing the expense of hiring a new person to replace the offending employee. As Zinder explains, "For first-party fraud, the expense of recovering from that would include lost capital, legal fees, the resources and time spent on investigations and training."



Generally, **5% of a company's total fuel spend is lost to fraud and misuse**. However, this will differ depending on the type of business you run. If you're a transportation and logistics company, fuel spend is going to be a significant percentage of your total expenses. If you're in one of the trades, fraud costs might be on the lower end of the spectrum because you're spending less on fuel. For trades businesses (such as plumbing, electrical, or general construction services) that use work vehicles (vans, pickups, etc.), fuel is still a major expense, but it generally makes up a smaller portion of the overall budget than for full-scale transport fleets. Regardless of how much you're spending on fuel, getting a handle on fraud should be a priority for fleet managers. Read on to learn just how much fraud is costing businesses.

The cost of fraud in the 2020's

Here's some data to illustrate just how much fraud is costing fleet businesses today. If you're running a 1,000-vehicle fleet with $5M in annual fuel spend and a $10M total operating budget.

Here's what you could be losing:

$250,000

PER YEAR ON $5M BUDGET

Fuel fraud/misuse may amount to up to 5% of the fuel budget — that's around $250,000 per year on a $5 M fuel spend.

20%

ESTIM. EXTERNAL FRAUD

Of that, internal misuse (driver/employee card misuse, unauthorized fill-ups, etc.) could account for 80% (=$200,000), while external fraud (card skimming, stolen credentials, etc.) might be 20% (=$50,000).

19–22%

OF TOTAL OPERATING SPEND

Looking beyond fuel — when maintenance, operations, and all spend are included — **industry surveys suggest losses from 19-22% of total operating spend**. On a $10M budget, that could mean up to $2 million annually.

Of course, actual losses will vary by fleet size, the level of control a fleet manager has optimized their card to exert, and sector. However, regardless of those factors, it is clear that although internal misuse typically represents the larger share of the problem, external fraud is increasingly becoming a meaningful risk that fleets must proactively address.





Beating fraudsters: The ultimate solution for fleet managers

Unauthorized use and skimming are important types of fraud fleets should focus on.

To best mitigate internal first-party fraud you should:

- Train your employees on what to look for and avoid
- Set up controls around driver spend
- Pair your fleet card with a telematics device to help you connect where your vehicles are and if they are the ones fueling
- Partner with your fuel card provider to help you put fuel card controls in place.

Read on to learn how AI is helping us all beat fraudsters at their game.

Partner with a fuel card provider offering fraud alerts

You may be concerned from time to time that fraudulent fuel card activity has occurred. In the past, you'd call your fuel card provider to validate any flagged transactions. In the past, you may have experienced long wait times on the phone with customer service. Recently, many providers have implemented new email and SMS alerts to help avoid these time-wasting customer service experiences. You can validate transactions directly by responding to the SMS or email alert, terminate cards suspected of fraud, and get legitimate drivers back on the road lickety-split.

Pair telematics with fuel card data to protect against fraud

There was a time when analyzing transactional data to surface any outliers was a time-consuming administrative burden, but necessary for fraud prevention. For today's fleet manager investing in a telematics program can help alleviate a lot of that burden. This is because when you pair telematics data with fuel card data you suddenly have quick and easy access to evidence of fraud. With these two tools working together fleet managers can protect against first- and third-party fraud. In some cases even catching fraud and misuse before it happens. This is all while increasing fleet manager confidence that purchases are within company policy and any fraud or misuse is kicked to the curb.

You'll hear tools like this in the marketplace called "telematics integrated fraud protection" or "one-click fraud protection." Think of it as a device in the vehicles sending data streaming real-time to your fuel card provider. The provider then enhances the authorization data to help prevent fuel card misuse.





Using AI to help fleet card customers manage fraud and overall operations more effectively

Nearly half (46%) of leaders are using more than ten individual tools to manage their operations with 30% saying it's too many to count. They toggle between an HR platform, a finance platform, a fleet platform, the list goes on and on. With that level of complexity, they are of course looking for ways to simplify their day-to-day. They also want to manage their fleet from where they are at any given point in time whether it be on the go, out in the field, or in the office. So what's the best solution when it comes to fraud protection? Fraud alerts can help, especially if they work speedily to let the fleet manager know of any issue, and if the alert system allows the fleet manager to react swiftly by clicking through a prompt.

With AI, fleet card customers can now manage fraud with a system that works as described above. WEX's Actionable Insights platform is an example of this kind of technological advancement powered by AI. With Actionable Insights, customers can automate driver alerts and other operational tasks tied to fraud protection. Alerts notify customers in real time about purchase controls exceeding limits, odd or unexpected activity, or a need to remind a driver to stay in compliance.

AI can be used to simplify a fleet manager's job and unburden them of tedious administrative tasks while also increasing the speed and effectiveness of fraud protection. Fleet card providers are developing AI tools that will change managers' approaches to managing fleets. With WEX's Actionable Insights, a fleet manager can easily engage with an AI-powered interface, which provides data-driven insights about driver behavior and much more. One can quickly and easily learn who's fueling at which station, when, and where the outliers exist.

With Actionable Insights fleets can pinpoint fraud in easy-to-read charts and graphs and effectively and efficiently determine trends. The insights tool gathers together a number of improvement opportunities, based on the data fed into the system. If the tool surfaces, say, 11 improvement opportunities, those are fed in order of priority to the customer a few at a time. Instead of overwhelming a fleet manager with 11 priorities, they're offered 1-3 of the most pressing suggestions. The tool explains the issue to the user. A common issue that would be flagged by Actionable Insights is a driver filling up three times the amount of gallons that his vehicle has capacity for at every stop. Misuse that might have otherwise gone unnoticed is highlighted automatically and presented to the fleet manager with a clear path toward a solution.

The tool not only identifies issues, but provides potential solutions. The tool can text that driver, the driver can be placed on notice, or their card can be suspended. Or, if it's not fraudulent activity the fleet manager can indicate that. The driver's purchase control limits could then be expanded so the tool does not alert the fleet manager again that this particular driver is fueling outside the norm, and the tool then moves on to the next item.

Fleet managers can automatically see the most pertinent data that in the past might have taken 10 hours to surface and analyze. The tool interacts with the fleet manager in natural language, answers questions, and presents data with a natural language explanation.

But then the tool also goes further, and suggests the number one recommended action to take to capitalize on the data provided. Suspend the card? Hit this button and the tool does the work for you. With AI tools like Actionable Insights, customers gain confidence and clarity and they also get back their most precious resource, which is hours in the day. They can manage these alerts as they arise, where they are, on the go.

AI for cleaner data

A large language model (LLM) machine learning tool like Actionable Insights is highly capable of data cleansing as well. As fleet managers know, there are a lot of different fuel providers in the U.S. with a whole variety of systems that are not standardized across providers. This means coding is not an exact science, and purchases are often miscoded, which creates unclean data. Here's an example: Let's say a driver purchases 32.2 units of something, and the system incorrectly labels it as Red Bulls. It's not likely that anyone would be purchasing 32.2 cans of Red Bull. It's not even possible to purchase a .2 can of Red Bull. This item has clearly been miscoded and the item likely should have been coded as a fuel purchase. Actionable Insights identifies such an error and corrects the data.

Catch the fraudster mid-action with AI fraud protection tools

Traditional fraud detection systems are slower and less effective. With traditional methods you're often detecting the fraud after the fraudster has run away with the cash—with AI and machine learning tools to protect against fraud in a lot of cases you see the fraudster in action before he has the chance to defraud the customer.

AI learns a fleet's patterns and picks up on anomalies

The most advanced AI fraud protection systems learn a fleet's patterns to detect and block suspicious activity before it happens. Unusual fill-up? Wrong state? The tool flags it and notifies you immediately.

How AI can help reduce false positives

The best fuel card providers now deliver machine learning transaction models to protect against fraud. Through machine learning, providers can track both driver behavior and geography. Then the AI model contemplates risk across thousands of dimensions and creates a probability score. Your provider can then use that probability score to decline a transaction in real-time. The value these models offer is the capture rate. What AI models have been effective at doing is increasing the precision of fraud detection. The result of the new technology is a reduction in false positives: fewer instances when an activity is mistakenly flagged as fraud. AI can also produce reactive pattern predictions.



If a fuel card provider declines a series of transactions the tool can then run those transactions through a data model and surface what are presumed to be false positives. The tool can draw hundreds of correlations a human may never be able to detect, and that information can then be used to generate alerts for customers. This helps keep drivers on the road, customers experiencing fewer operational problems, and drivers and fleet managers experience fewer headaches.

Traditional fraud protection versus AI-powered fraud protection

Here's the difference between conventional fraud prevention and AI-powered fraud prevention. Twelve to eighteen months ago, using conventional tools, fuel card providers were alerted when there was a suspicious fuel card swipe. A human opened the alert notification. A Fraud Analyst rep found the customer and sent them an email. The fleet manager on the receiving end of that email would then comb through pages and pages of data looking for the anomaly — it was a multi-step process that sometimes created tremendous wait times. With automation tools using AI and machine learning now the end-to-end alert process takes approximately five minutes. A year ago, using conventional fraud prevention methods, this kind of process took an average of seven days. Implementing AI machine learning fraud controls completely changed how fuel card providers interact with customers and how quickly fleets can get drivers back on the road.

These fraud prevention technologies are detecting and preventing fraud in real-time, in application flows, and in transaction flows at both the point of pre-authorization and the point of post-authorization.



The benefits of a closed-loop network when it comes to fraud

The strongest purchase controls are possible when your fleet card provider operates within a closed-loop network. A closed-loop network provides control over misuse or unauthorized spending and improves expense management through Level III data on 99.8% of transactions, which open-loop systems can't offer. Level III data is the most detailed information available, typically referring to the line-item breakdown of a commercial credit card transaction.

A closed-loop network is a payment arrangement where one entity acts as the card issuer, the payment processor, and the network operator providing customers with granular purchase control. Customers can choose to control various variables: they can place spending limits on what drivers spend on oil and fluids, quick lubes, car washes, roadside assistance, general merchandise, labor, and/or parts and service.

An open-loop network (think Visa or Mastercard) is a payment system that facilitates transactions between accounts at different, unaffiliated financial institutions and is accepted by a broad, universal network of merchants globally.

One of the benefits of a closed-loop network is that it allows customers the advantage of Level III data. Level III data gives the most detailed information available in the line-item breakdown of each fuel card transaction. With an open-loop network, far less detail is available to the business.

With a closed-loop network you have:

- The ability to block convenience store purchases, even when drivers pay for fuel inside (something open-loop cards can't do).
- Detailed, itemized transaction reporting with Level III data for enhanced visibility and decision-making on 99% of transactions.

A closed-loop network gives customers a distinct advantage when it comes to fraud protection. At the end of the day, it's not just about reducing fraud. It's about optimizing driver uptime, controlling costs, and maximizing profitability.



What steps should an organization take to recover from a fraud attack?

There are a variety of steps organizations should take to recover from a fraud attack. It starts with setting company spend and expense policy upfront and training employees on the right behaviors. For more control, a fuel card can help you as well. For example, with a fuel card, you can:

- **Set and enforce policies to prevent misuse—**With some fleet card companies, you get customizable spend controls so you can not only dictate who can use your cards, but how and when they can be used. This gives you ultimate protection and control over every transaction, including:
  - Placing a spend limit on purchases
  - Restricting spending categories to fuel only or expanding to include maintenance and c-store transactions
- **Control usage times—**Restrict transactions to specific hours of the day or days of the week
- **Set spending limits—**Cap spending per day, week, or transaction
- **Manage transaction frequency—**Limit the number of transactions per day or week
- **Enforce fueling limits—**Define maximum gallons per day to prevent misuse

Additional tips for staying on top of fraud

Here are some additional tips for staying on top of fraud:

- File your fraud disputes in a timely manner
- Stay vigilant on reports and receipts
- Prevent the fraud up front by setting your company spend and expense policies and driving compliant behaviors and making them front and center.
- Train your employees on the company spend policy on a regular basis
- Fuel card products can help combat third party fraud. For example, with WEX fuel cards, fewer than 1 in 12,000 transactions were fraudulent in one 60 day period. That's less than 0.01% of total transactions, so if you are a WEX customer your fuel card use has strong fraud protections in place to help protect your business.

The future fleet manager will look for a fuel card provider backed by advanced technology and stores of data who also serves as a trusted advisor and a steady resource continually surfacing real-time insights and solutions.

> Our AI learns from the massive volume of transactions flowing through our system, delivering faster, smarter fraud protection."
>
> **Cecile Zinder**
> *Vice President of Product at WEX*

Why WEX for the best fraud protection in the business

When it comes to fighting fraud, customers don't just need a product — they need a true partner. WEX doesn't just hand them the tools, they stand beside them with the expertise, insights, and data intelligence to help outsmart fraud at every turn. It's a partnership built on trust, proven by experience, and designed to keep businesses moving with fewer disruptions and more control.

Because WEX has been in the business for over 40 years and has long-standing relationships with thousands of businesses, it is afforded a more comprehensive answer to fraud protection. WEX processes over 30 million transactions a month, across approximately 95% of U.S. fuel stations, providing its AI with the data it needs to learn and adapt, making it smarter than generic, off-the-shelf fraud tools you might see with other systems in the marketplace today. Zinder says, "Our AI learns from the massive volume of transactions flowing through our system, delivering faster, smarter fraud protection."

WEX's AI-powered solution, built from years of experience and fleet insights, detects and can prevent fraudulent transactions in real-time. It uses AI and telematics data to identify suspicious patterns, instantly flagging discrepancies in location, purchase type, and time of day. This multi-layered approach has already proven highly effective, detecting over 20,000 fraudulent transactions and saving our customers millions in potential losses in Q1 of this year alone. Zinder says, "We also keep humans in the technology loop and use reinforcement learning models to make sure our insights are getting better with time and will always grow with our customers."

Very few companies have the reach and history that WEX has with fuel providers in the U.S. Because of that 40+ year history, WEX's team understands the variety of systems in the marketplace. Additionally, because of the longevity of the company, WEX has many years of proprietary data, so out of the gate WEX is already leading by feeding its AI with extensive knowledge. As a result, cleansing and normalizing a broad range of data means that inconsistent purchase codes and non-standard data that's across the merchants and fuel networks gains consistency quickly and easily.

WEX also has an end-to-end enterprise fraud risk platform for the purpose of protecting against third-party fraud. This is done via transaction monitoring using AI. If suspicious activity occurs during a fuel card transaction, that transaction is declined. Customers can choose what rules they'd like to have applied, whether they prefer location, type of purchase, or time of day of purchase to spark a declined charge. By coupling automation, data-driven insights, and secure digital payment methods like virtual cards, WEX helps customers improve their bottom line and fortify their security posture.





Conclusion

As fraud tactics evolve, fleet managers are facing more complex and persistent threats than ever before. But the same technologies that have enabled fraudsters are also empowering businesses to defend themselves more effectively. By combining clear company policies, strong purchase controls, telematics integration, and AI-driven insights, fleets can move from a reactive posture to a proactive one—detecting suspicious activity earlier, reducing false positives, and stopping fraud before it impacts operations. The result can be not just fewer fraudulent transactions, but greater confidence, improved driver uptime, and stronger financial control across the fleet.

The future of fleet fraud protection will belong to organizations that pair smart technology with experienced partners. With advanced AI capabilities, decades of industry expertise, and access to one of the largest sets of fleet transaction data in the world, WEX helps businesses turn fraud protection into a strategic advantage. Instead of spending hours chasing anomalies or investigating suspicious activity, fleet managers can focus on running more efficient, profitable operations—knowing the right systems are in place to keep fraudsters one step behind.



WEX is a leading, global fintech solutions provider, simplifying payments and back-end business processes in the fleet management, benefits management, and corporate payments areas. To learn more, please **visit the company's About WEX page.**

Sources

USA Today

Pew Research Center

Whyy

Scripps News

Mashable

Yahoo Finance

Fraud.org

Federal Trade Commission

Copyright ©2026 WEX Inc. All rights reserved. The information in this document is subject to change without notice.

2874374016 (05/26)