

Fleet card fraud: Assessing the impact of fuel fraud on profitability

Motive × **FREIGHTWAVES**



Contents

3 Overview

Key insights

4 Operators still blind to cost saving opportunities

7 Fraudulent fuel spend, a hidden cost center

11 Current fraud detection solutions waste time

13 More could be done to combat fraud

15 Conclusion: Breaking down silos between fleet card spend and management

16 Key suggestions

17 About the respondents

18 About the partners

Overview

2022 marked a worrying record for the trucking industry: It was the costliest year to conduct business for fleet operators, [surpassing](#) the record established in 2021. Price hikes were especially noticeable when it came to fleet expenses, most notably fuel costs, followed by lease or purchase payments, repair and maintenance costs, and insurance premiums.

Fleet operators work around the clock to keep pace with these rising expenses, but the fraudulent fleet card activity that plagues the industry creates an additional burden. Spotting and preventing fraud presents an opportunity to realize savings, but due to outdated

solutions and disparate vehicle management and fleet card management systems, fraud can slip through the cracks undetected. Fraud – intentional stealing – is shrinking profit margins and increasing overhead and total cost of operation amid a hostile economic environment.

FreightWaves and Motive teamed up to survey fleet operators about their operations costs, especially concerning the extent to which fraud impacts their bottom lines, how their companies are fighting back and with what success.

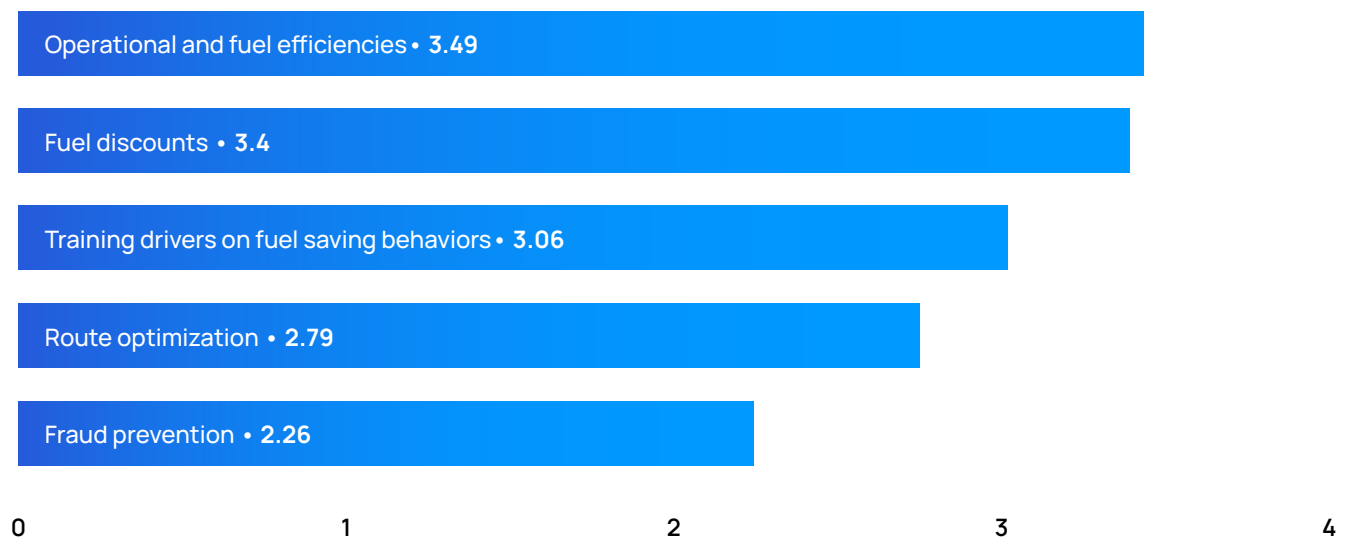
Key insights

- Nearly 55% of fleet operators say they struggle to detect fraud.
- Over half of fleet operators with 200+ vehicles spend more than 10% of their time dealing with fleet expenses.
- 49% of operators estimate up to 5% of their fuel spend is fraudulent.
- 45% of fleet operators believe third-party fraud impacts them the most.
- Manual monitoring and paperwork are the most time-consuming aspects of fraud prevention for 47% of respondents.
- 70% believe their company could be doing more to combat fraud.

Operators still blind to cost saving opportunities

From 2021 to 2022, the average cost of fuel per mile for fleet operators surged by 54% as fuel prices peaked in June 2022, according to the American Transportation Research Institute's (ATRI) ["An Analysis of the Operational Costs of Trucking."](#) Fuel still remains the largest vehicle expense fleet operators contend with, but companies still lack efficient and impactful ways to counter costs that are again rising to rival 2022 levels.

What methods do you find the most effective in combating rising fuel expenses?



Fleets see operational and fuel efficiencies followed by fuel discounts as the most effective ways to lessen the impact of rising fuel expenses. In contrast, fleet operators don't find fraud prevention effective. Is this truly reflective of the savings opportunities presented by each solution, or is it because fleet operators struggle to implement fraud prevention processes and technologies that deliver a return on investment?

What main challenges do you face in managing your fleet expenses today?

Identifying operational savings • 64%



Detecting fraud • 55%



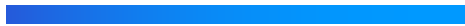
Spend control • 53%



Outdated technology or processes • 28%



Lack of shared data between fleet and spend platforms • 25%



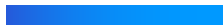
Managing multiple cards and platforms • 21%



Limited discounts • 15%



Poor customer support • 13%



Hidden fees • 8%



Calculating taxes • 4%



Detecting fraud is an issue for almost 55% of fleet operators. Even though it's one of their top pain points behind identifying operational savings, it is likely that fraud prevention is an operational blind spot because it's so difficult to address with current processes. Why is it so challenging for operators to identify operational efficiencies and detect fraud?

How much of your company's time is spent managing fleet expenses (e.g. fuel, maintenance, reimbursement, IFTA taxes, compliance, etc.)?



Less than 5%

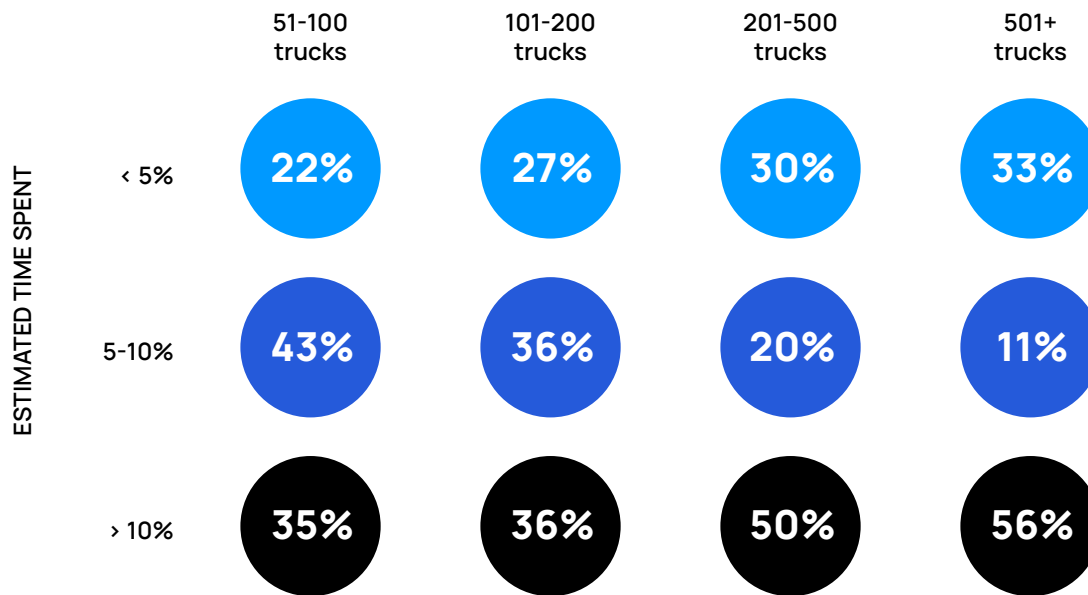


5-10%



More than 10%

How much of your company's time is spent managing fleet expenses (e.g. fuel, maintenance, reimbursement, IFTA taxes, compliance, etc.)?



Managing company expenses is time-consuming and cumbersome due to outdated processes, requiring intense resources. Nearly 42% of respondents spend more than 10% of their company's time managing fleet expenses, and it's even more common among larger fleets. Companies with more than 200 vehicles report

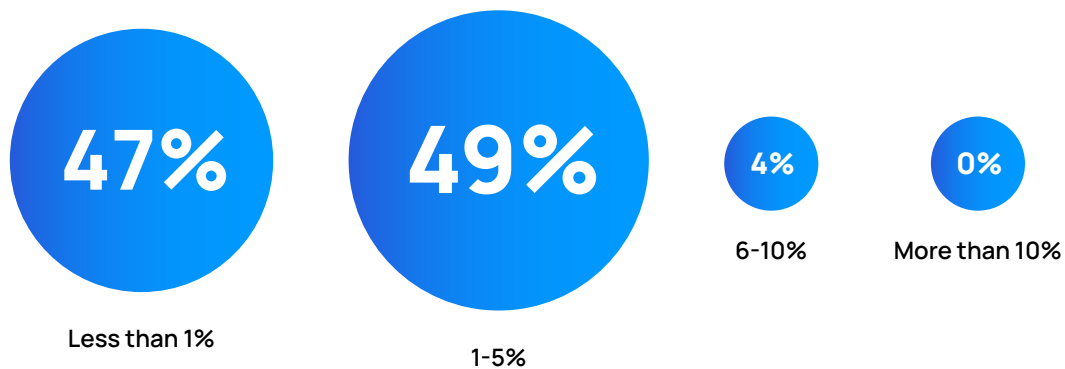
spending greater than 10% of their time dealing with fleet expenses.

These lost hours and dollars are a result of a lack of efficiency, and fraud prevention is one of the most overlooked opportunities for improvement.

Fraudulent fuel spend, a hidden cost center

High fuel prices don't only mean trouble for fleet operators' pocketbooks, but they also provide a strong incentive for theft and misuse of cards. Fraud prevention is a cost-saving opportunity that operators can no longer afford to ignore.

What percentage of your fuel spend do you estimate is fraudulent?



Fraud has a substantial impact on operating costs. In this survey, nearly half of respondents (49%) believe that 1%-5% of their fuel spend is fraudulent. Though this number may seem small, let's consider quantifying what 5% looks like based on numbers in the ATRI's 2023 [report](#). The average number of miles driven annually per

tractor-trailer is 78,863. If you multiply this by the average fuel cost per mile, 64.1 cents, it would equate to roughly \$50,551 in fuel spending per truck per year. For a fleet with 200 trucks, that would be a total fuel expenditure of approximately \$10,110,237.

78,863*

Average miles driven annually per tractor-trailer truck

\$50,551

Fuel spend per truck per year at \$0.641 per mile

\$10,110,237

Estimated annual fuel expenditure for 200 truck fleet

In this scenario, since fleet operators assume as much as 5% of their fuel spend is fraudulent, that would mean they would need to budget an additional \$505,512 for anticipated fraud losses.

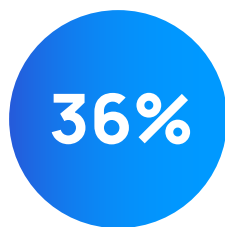
5% OR \$505,512

Estimated annual losses due to fraudulent fuel spend

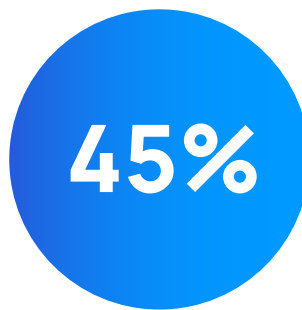
*Based on numbers in the ATRI's 2023 report

There are multiple forms of fraud that can contribute to that cost, originating within and outside of the company.

What type of fraud do you believe is most prevalent in your company and contributing to the cost of operating your fleet?



Third-party fraud
(i.e. skimming, scams or phishing)



Employee "friendly-fraud"
(i.e. drivers inflating miles/ transactions, side fueling/ siphoning, multiple pump transactions)



Out-of-policy spend
(i.e. personal expenses, sharing cards)

In this survey, fleet operators were asked about out-of-policy spend, employee “friendly fraud” and third-party fraud. Weak security measures and a lack of integrated fleet card management and vehicle management contribute to challenges in handling all types of fraud.

Out-of-policy spend

Out-of-policy spend refers to employee purchases of goods or services that violate a company expense policy, usually for their personal use.

Example: A company provides an over-the-road truck driver with a fleet card. His company's policy permits him to purchase fuel and truck-related items and services. He stops at a truck stop, purchases fuel at the pump and then walks inside the store, where he buys snacks using the company fleet card. The driver has broken company policy. Staff don't catch the small but out-of-policy transaction until weeks later on the card statement. Although it was an authorized merchant, the company's fleet card does not permit setting eligible purchase categories to restrict this spend.

Employee “friendly fraud”

Employee “friendly fraud” in this context refers to employee misuse of a company card for his or her personal benefit and attempts to disguise the wrongdoing.

Example: After leaving the yard, a truck driver drives the company van a mile home to pick up personal gas cans. He then goes to a gas station to fill those cans using the company's card. Once the cans are full, the driver heads to a remote area, uses the gas to fill up his friend's car and then resumes his assigned route. To back-office staff with no way to easily track fuel tank levels, the fuel stop looks routine and the misuse of the card is never detected.

Third-party fraud

Third-party fraud as it relates to fleet cards occurs when someone outside the company gains access to card data and uses it for personal gain, which can happen through sophisticated means such as skimming, scams or phishing.

Example: A driver stops at a truck stop to refuel. Unbeknownst to him, a card skimmer has been installed on the card reader and keypad on the fuel pump. The driver pays as normal and fails to notice it takes extra effort to enter the card's PIN due to the phony keypad that the scammer installed. A few weeks later, when a fleet operator employee is performing a manual check of the driver's GPS locations against his fleet card report, she notices that suspicious online charges have appeared on the card statement. This is a red flag because the policy only allows the driver to use the card for fuel and maintenance.

A significant 45% of all respondents believe that third-party fraud, such as skimming, scams or phishing, is the most prevalent type of fraud contributing to fleet operation costs. We see this increasing concern for third-party fraud as fleet sizes increase, with 60% of fleets with 201-500 trucks and 78% of fleets with more than 500 trucks being concerned about third-party fraud.

Although fleet operators have deployed fraud prevention measures, they experience varying degrees of success in detecting it.

Current fraud detection solutions waste time

As the fraud arms race heats up and continues to plague the industry, more fleet operators have adopted fraud prevention measures into their business strategies.

Which of the following fraud prevention measures has your company taken to mitigate fuel theft and control/protect spend?

Using spend controls • 59%

Automated systems that give visibility into suspicious transactions • 59%

Training driver/fleet management on fraud prevention • 40%

Manual fraud monitoring (i.e. paper forms) • 32%

AI and telematics-based fraud prevention • 26%

Third-party consultants/auditors • 11%

In this survey, 58% of fleet operators report using spend controls as a common fraud prevention tactic. Spend controls can be turned on through fleet card management platforms, allowing companies to set standards on how cards can be used and who can use them, helping them stay within budget and lessen the chance of fraud. Guardrails can be set on the hours cards are active or the categories of goods or services that can be purchased. Phone-based unlocking and blocking specific merchants are also features that can empower companies to increase security beyond what an easily shareable PIN code can offer.

Automated systems providing visibility into suspicious transactions are also important tools that 58% of respondents use to help stop fraud in its tracks. While companies recognize the value of automated fraud alerts, their benefits are limited if the systems are disconnected from other critical telematics data. This seems to be the case for the 74% of respondents who aren't currently using AI and telematics-based fraud prevention.

What aspects of your current fraud prevention measures do you find most complicated or time-consuming?

Manual monitoring and paperwork • 47%



Training staff on fraud detection • 36%



Setting up spend controls and tracking cardholders to spend • 34%



Adopting new technologies or processes • 34%



Managing multiple cards and platforms • 23%



While many companies utilize automation in their fraud prevention measures, manual monitoring and paperwork are still a time-consuming problem for the near majority (47%) of respondents.

Even most modern solutions leave a gap between fleet card management systems and vehicle management systems because operators use decentralized methods with data silos. Paper processes, spreadsheets and human effort are currently the connector between

the two to compensate for the lack of integration. This means manually comparing fuel purchase locations to telematics data like vehicle location and fuel gauges.


These efforts are costly in terms of missed insights due to human error, but also because they are inefficient, with companies paying employees for the time spent doing these manual tasks when their focus could be elsewhere.

More could be done to combat fraud


Though the majority of fleet operators in this survey have some processes in place to prevent fraud, many also see these current practices as insufficient to tackle the full scope of the problem.

Do you believe your company is doing enough to combat fraud currently?

No, our company could be doing more • 17%



Somewhat, but our company could be doing more • 53%




Yes, our company actively invests in fraud prevention • 30%




A minority of respondents, 30%, believe their company is actively investing enough in fraud prevention, which means 70% believe their company could be doing more.

If "somewhat" or "no," what is preventing your company from investing in fraud prevention solutions?


Our company hasn't prioritized fraud prevention • 53%




Our company doesn't have time or resources • 39%



Other • 6%




Our company doesn't have the budget • 3%




The majority of respondents (53%) indicate that their company hasn't prioritized fraud prevention as a key issue. About 39% cite a lack of time or resources as holding the company back. Two respondents provided unique insights: "unaware of options" and "the thieves are very sophisticated and difficult to detect."

Which of the following fraud prevention measures do you plan to leverage in the future?

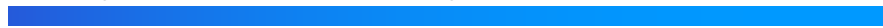
Driver and operational training measures on signs of fraud • **49%**



Integrating fraud software or technology into our fleet management platform • **47%**



Investing in AI and automated technologies for proactive fraud detection • **42%**



Adopting new payment platforms with advanced security features • **38%**



Leveraging third-party specialists and auditors • **11%**



Nearly half of the respondents (49%) plan to focus on driver and operational training to recognize signs of fraud. Close behind, 47% intend to integrate fraud software or technology into their fleet management platforms. About 42% are considering the use of AI and automated technologies for proactive fraud detection, which is a positive sign that companies are taking steps to reduce their manual processes.

While telematics data has become an integral part of fleet management, companies are still missing out on the value of integrating their fleet card management systems. By managing fleet and fuel spend together on one centralized dashboard, companies would gain valuable 360-degree insights, save money and get hours back due to reduced overhead.

Conclusion: Breaking down silos between fleet card spend and management

As third-party fraud, out-of-policy spend and employee fraud continue to drain fleet operators' bottom lines, companies are recognizing the necessity to put controls in place. However, many still struggle with implementing an efficient solution to handle the problem. They rely on the same processes they have used for years, using disconnected systems and human effort to draw the line between fleet card and vehicle management, which is time-consuming and leaves room for error.

FreightWaves asked respondents what fraud prevention methods they plan to leverage in the future. The responses reveal a strong inclination toward:

- + fleet and expense management solutions
- + AI and automated technologies
- + adopting payment products with advanced controls and security

Respondents also recognize the need to train drivers and fleet managers on detecting fraud and underscored the prevalence of various types of fraud they are facing.

An increased inclination toward fleet and spend integrations and automation tools suggests the desire for simplifying fraud detection methods as a reliance on manual processes continues to under deliver.

As we learned from the report, respondents recognize fraud detection as a substantial pain point in managing their fleet expenses, and many respondents feel delayed investments are due to company reprioritization.

While respondents also recognize that fraud is impacting their financial operations, they believe detecting it is the least effective way to combat rising fuel expenses, despite the fact that the majority believe up to 5% of their fuel spend is fraudulent.

This suggests that because companies find fraud detection to be difficult to identify and feel their solutions do not give them the visibility they need to reduce it, operators do not realize the full potential of this cost-saving center.

For fleet operators, these insights shed light on vast potential for investment in integrated technology and more secure payment products that leverage shared fleet and spend data. Embracing these fraud management trends can also significantly contribute to lowering overall costs of operation, improve employee experiences and reduce operational inefficiencies.

Key suggestions

1. Obtain near real-time fraud detection alerts. This AI technology feature is instrumental in proactively reducing fraud. The majority of respondents still rely on manual processes, even though there is a high degree of dissatisfaction, and leave organizations vulnerable to identifying threats weeks or months after they have already had a financial impact.

2. Implement phone-based unlocking features. Phone-based unlocking enhances security by adding layers of protection compared to PIN codes. It reduces third-party and friendly fraud risks, as PINs are vulnerable to capture by cameras and skimming devices. Additionally, this functionality offers better control during point-of-sale transactions when cardholders need to unlock their phones for spending.

3. Adopt advanced spend controls that offer more security. Over half of respondents already use spend controls as a fraud prevention tactic, however, one-third still find setting up spend controls to be complicated and time-consuming. To rectify this, operators should aim to partner with providers that allow for easy-to-use, granular spend control capabilities, including controls over merchant, time of day and location that are intuitive to deploy, customize and automate.

4. Integrate vehicle and fleet card management into one platform for better operational and fuel-efficiency savings opportunities. Over half of respondents cite identifying operational inefficiencies and detecting fraud as some of their greatest challenges in managing their fleet expenses. By managing fleet and fuel spend together on one centralized dashboard, fleet operators would gain valuable 360-degree insights, save money and get hours back due to reduced overhead.

5. Reduce fraud by investing in better telematics-backed security features and reporting capabilities.

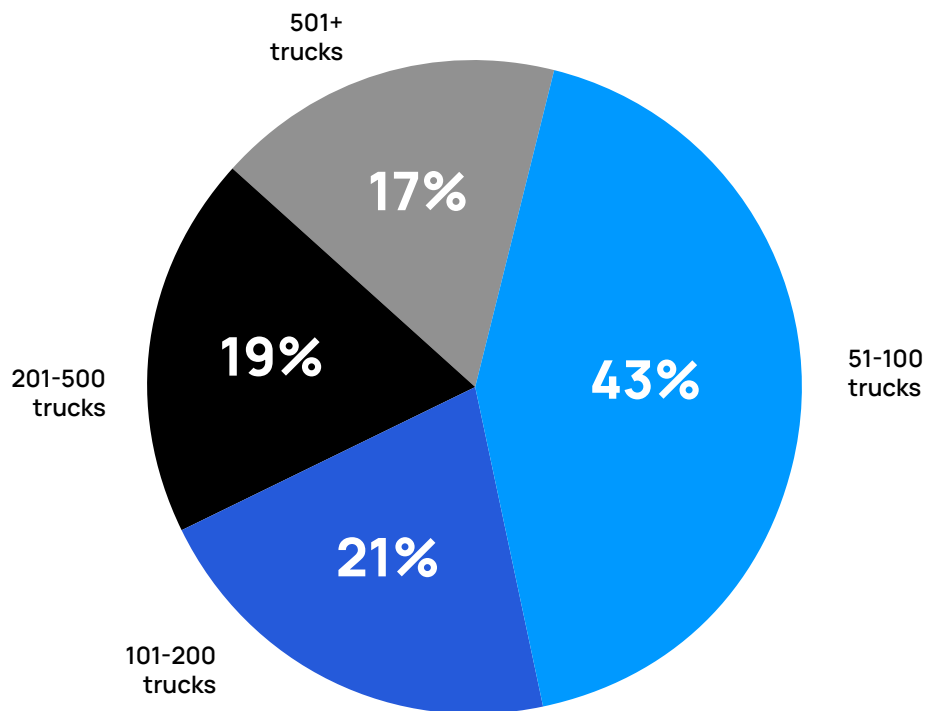
Even though half of respondents have deployed some degree of automation to detect suspicious transactions, they believe reducing fraud would have the least impact on lowering their fuel expenses, even though most believe up to 5% of their fuel spend is fraudulent. This suggests current fraud management processes are not leveraging fleet and spend data points to uncover these cost savings.

6. Train driver and fleet management fraud detection practices. Respondents agree that employee training could help mitigate fraud threats and the majority believe third-party fraud is the most prevalent threat to their operating expenses. Third-party fraud is sophisticated and always changing, making it critical for drivers and fleet managers to be aware of the types of threats they experience and how to identify them, including card skimmers, phishing emails and more.

7. Consolidate cards and expense platform management. Nearly a quarter of respondents cite managing multiple cards and platforms to be time-consuming or complicated. Incorporating multiple payment products across multiple platforms can increase a company's exposure to fraud, and create time-intensive processes. Fleet operators who adopt a single fleet and spend management solution can elevate a company's fraud management performance while reducing overhead.

About the respondents

What is your company's fleet size?



The survey focused on fleets ranging from 51 trucks to 501 and above. Companies with fleet sizes ranging between 51-100 trucks were the most common at 43% of respondents, followed by 21% coming from fleets with 101-200 trucks. The largest fleets – 201-500 and 501-plus trucks – are less common, making up about 19% and 17% of responses, respectively.

About the partners

motive

Motive empowers the people who run physical operations with tools to make their work safer, more productive, and more profitable. For the first time ever, safety, operations and finance teams can manage their drivers, vehicles, equipment, and fleet related spend in a single system. Motive serves more than 120,000 customers – from Fortune 500 enterprises to small businesses – across a wide range of industries, including transportation and logistics, construction, energy, field service, manufacturing, agriculture, food and beverage, retail, and the public sector. Visit gomotive.com to learn more.

FREIGHTWAVES

FreightWaves is a price reporting agency focused on the global freight market and the leading provider of high-frequency data for the global supply chain. FreightWaves' price, demand, and capacity data allow customers to benchmark, analyze, monitor, and forecast the global physical economy. Visit freightwaves.com to learn more.