RISK INSIGHTS

UNDERSTANDING AND PREVENTING FLEET FRAUD

Fleet fraud refers to a host of deceptive activities that may occur amid the sale and operation of commercial vehicles and their individual assets (e.g., engine parts). Such fraud is a significant concern for any business that utilizes commercial vehicles, whether it's a few small cars or a dozen tractor-trailers. According to a recent report from trucking software company Motive, as much as 22% of the average business's fleet spend is compromised by vehicle theft and fraud. Furthermore, 44% of business owners confirmed that fleet fraud affects their operations, yet they don't know how to address it.

Fleet fraud not only leads to financial losses and elevated insurance expenses but can also reduce operational efficiencies and threaten roadway safety. As such, it's imperative for businesses and their commercial drivers to be aware of such fraud and related mitigation measures. This article explores the five main types of fleet fraud—vehicle theft, cloning, title washing, staged accidents and fuel fraud—and provides effective prevention strategies.

1. VEHICLE THEFT

The FBI defines vehicle theft as the unlawful possession or attempted taking of a vehicle without the owner's or designated operator's consent; it occurs approximately every 44 seconds in the United States. Vehicle theft is a prevalent form of fleet fraud, often orchestrated by organized crime groups. Stolen vehicles may be shipped to different black markets overseas, stripped for parts at chop shops or resold to unsuspecting consumers.

Despite efforts to recover stolen vehicles, a substantial number of criminals remain at large, leaving affected businesses with prolonged operational disruptions, fleet replacement challenges and complex insurance claims. Following vehicle theft incidents, businesses may also face ongoing financial challenges, reputational damage, and additional coverage restrictions and premium costs.

Several steps can help businesses minimize vehicle theft among their fleets, such as:

- **Employee education**—Commercial drivers should receive training on basic vehicle security measures, including parking in secure and well-lit areas, locking the doors and closing the windows before exiting vehicles, and never leaving vehicles unattended with the keys in the ignition (if applicable).
- **Theft deterrents**—To help dissuade potential thieves from targeting them, all vehicles should be equipped with alarm systems, wheel locks, theft-deterrent decals and window etching.
- **Vehicle immobilizers**—Besides theft deterrents, certain systems (e.g., fuse cut-offs, kill switches, and ignition and fuel disablers) can help immobilize vehicles that have been stolen or are in the process of being stolen, rendering them useless to thieves.
- **Tracking technology**—When vehicles are stolen, time is of the essence to ensure prompt recovery and minimal damage. Installing tracking technology within vehicles can make them easier to locate if they end up in the wrong hands and emit signals to local law enforcement and vehicle monitoring agencies, allowing for extra assistance.

2. CLONING

Vehicle identification number (VIN) cloning involves assigning a stolen vehicle the identity of a legally owned vehicle with a similar appearance. It's a sophisticated crime that thieves can launch by taking photos of legitimate vehicles' VIN plates while they are stationed in parking lots, at rest stops or along the roadway. From there, thieves can create counterfeit VIN plates for stolen vehicles of similar makes and models before illegally selling them to unsuspecting consumers.

Upon discovering VIN cloning, law enforcement agencies generally seize the stolen vehicles and return them to their original owners, leaving those who were scammed into buying these vehicles with nothing and forcing them to continue making any loan payments attached to their purchase. Recent research from the National Crime Prevention Council revealed that up to 225,000 stolen vehicles are subject to VIN cloning every year, contributing to at least $36 million in fraudulent transactions since 2001. Consequently, businesses could encounter serious financial fallout if any vehicles in their fleets are compromised by VIN cloning.

To prevent cloning concerns, it's best for businesses to uphold these measures:

+ **Secure purchase protocols**—Businesses should conduct plenty of research and engage in proper vetting before purchasing new and used vehicles for their fleets. This involves verifying the vehicle's VIN plates with the appropriate government agencies and motor vehicle departments, carefully reviewing its accident and repair history, and scrutinizing past ownership patterns. Additionally, businesses should be wary of vehicle prices that seem uncharacteristically low or otherwise too good to be true; this is often an indicator of a fraudulent sale.

+ **Adequate fleet management**—Businesses should also designate trusted employees to be in charge of their fleet management operations and train them on sufficient vehicle purchasing, maintenance and security tactics. All fleet management practices should be well documented.

3. TITLE WASHING

Some natural disasters, namely hurricanes and floods, can cause extensive damage to vehicles due to prolonged water submersion. Although water-damaged vehicles should be rendered inoperable because of their compromised engines, they are often dried and cleaned, then sold in regions unaffected by the natural disaster without disclosing the damage—a practice known as title washing. According to vehicle data provider CarFax, as many as 800,000 U.S. vehicles have washed titles.

Businesses scammed by title washing may end up with unreliable and inefficient vehicles that require frequent maintenance and costly repairs, driving down overall fleet performance and productivity levels. What's worse, commercial drivers who operate vehicles with washed titles could be increasingly vulnerable to unexpected breakdowns and related accidents behind the wheel, hurting themselves and other motorists in the process.

Various measures can help businesses protect against title washing, including:

+ **Solid dealership connections**—Businesses should form strong relationships with trusted and reputable vehicle dealerships in their areas and only purchase vehicles for their fleets from these locations, thus mitigating the risk of fraudulent transactions.

+ **Ample inspection procedures**—Prior to finalizing vehicle purchases, businesses should have experienced auto mechanics conduct in-depth inspections, looking for any signs of water damage (e.g., water stains, sand or silt buildup, and mold and mildew growth). Businesses should also review all vehicle title and past ownership documentation to confirm its legitimacy.

RISK INSIGHTS

4. STAGED ACCIDENTS

Staged accidents are orchestrated by criminals to submit fraudulent insurance claims. Examples of such accidents include a driver slamming on their brakes with the intention of getting rear-ended by the vehicle behind them or a driver purposely sideswiping another vehicle. These scams often involve multiple participants, including additional vehicle passengers, unethical lawyers and deceptive medical providers. Together, scam participants typically inflate accident claims with false witness statements, nonexistent injuries and overexaggerated vehicle repairs, hoping to secure large insurance payouts.

In addition to endangering their commercial drivers and fleets, staged accidents can entangle businesses in complicated insurance claims and exacerbate their total coverage expenses, resulting in higher rates for the foreseeable future. In fact, industry experts estimate that these scams cost the insurance industry up to $20 billion annually.

To help mitigate staged accident risks, businesses should implement these strategies:

- **Defensive driving policies**—Commercial drivers should be required to follow defensive driving techniques, as this can make it more challenging for them to be targeted in staged accidents. These techniques include continuously scanning the road ahead for potential hazards, paying attention to posted safety signage and message boards, upholding applicable traffic laws, and maintaining an appropriate distance between surrounding vehicles to permit ample braking time.
- **Effective reporting measures**—If staged accidents occur, detailed and prompt reporting can reduce the likelihood of inflated insurance claims and associated payouts. Businesses should instruct commercial drivers to call the local police at the scene of an accident and file an in-depth report, taking as many pictures and videos as possible to document the damage. Drivers should also be discouraged from immediately admitting fault in an accident; instead, they should provide all relevant details and allow for a full investigation to take place.

5. FUEL FRAUD

Fuel fraud is a common issue in fleet management, usually involving employee misuse of business resources intended for fueling commercial vehicles. For instance, drivers may make unauthorized purchases using their assigned fleet fuel cards or siphon fuel from tanks or storage facilities for their personal vehicles. Drivers may also manipulate mileage claims in vehicle reports and related documents in an effort to conceal their deceptive activities.

Fuel fraud can carry a number of consequences, significantly distorting businesses' fleet data and budgeting and, in severe cases, threatening their overall profitability. According to the NAFA Fleet Management Association, such fraud can drain as much as 12% of businesses' total fuel spend, posing considerable financial challenges over time.

Multiple tactics can help businesses better identify and respond to fuel fraud, such as:

- **Fuel management practices**—Businesses can utilize advanced vehicle technology and software systems to track fuel consumption and detect abnormal activity in real time, catching fraudulent employees at the pump. In conjunction with these systems, businesses should diligently review all fuel transactions and ensure related purchases properly align with documented vehicle usage and fleet operations.

RISK INSIGHTS

- **Employee vetting and training**—Businesses should only hire trusted and experienced commercial drivers. This involves conducting sufficient background checks on job applicants and reviewing their work history for previous instances of fraud. Once hired, commercial drivers should be required to attend regular training sessions on fueling best practices and reporting mechanisms for suspicious behaviors exhibited by co-workers at the pump.
- **Fuel card restrictions**—To avoid unauthorized purchases on fleet fuel cards, businesses should deploy several controls, including personal identification numbers for each card, maximum transaction limits, and purchase restrictions based on driver profile and vehicle type.

CONCLUSION

Fleet fraud poses a major threat to businesses, but it can be effectively managed with proactive measures. By implementing robust security protocols, conducting thorough vehicle inspections, monitoring fuel transactions and educating drivers on fraud prevention, businesses can protect their assets and reduce the risk of fraud.

Businesses don't have to navigate this issue alone. Continued collaboration with trusted insurance professionals and organizations such as the **National Insurance Crime Bureau** can help further enhance fraud prevention efforts, ensuring a safer and more secure fleet management environment.

Contact us today for more commercial fleet resources and risk management guidance.