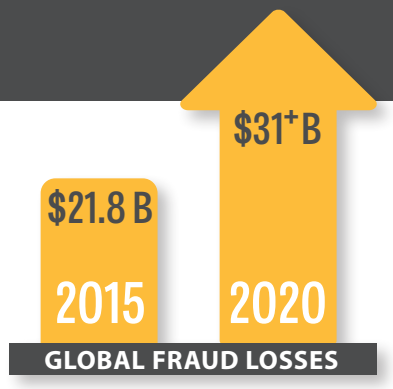
The Changing Nature of

FLEET CARD FRAUD:

Sources, Trends and Prevention

FLEET CARD FRAUD—RISKS AND SECURITY



Technology has led to rapid innovation in payment tools and methods. However, it has also created more opportunities for criminals to commit fraud.

Payment cards, such as fleet cards, are an especially attractive target. In 2015, global losses from fraud on credit cards, debit cards, and prepaid cards topped $21.8 billion.[1] According to industry projections, fraud losses will exceed $31 billion by 2020.

Realizing that even a single fraudulent transaction can have potentially devastating, long-term consequences, managers are constantly working to better understand how, where, and when fraud happens—from both inside and outside of their organizations. And, although it is difficult to predict what portion of this fraud will involve fleet card abuse, many fleet professionals are taking action to identify and rectify instances of fraud as quickly and effectively as they can.

There has been a tremendous amount of research conducted and awareness raised about consumer credit card fraud, but many of the conclusions don't necessarily apply to the fleet space.

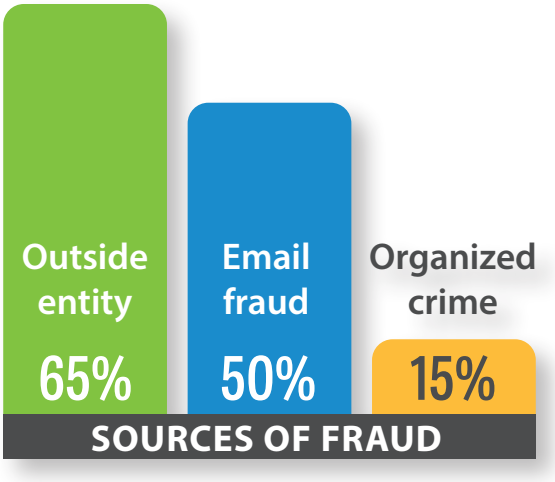
The purpose of this paper is to develop a better understanding of bank card vs. fleet card fraud, including:

- Why fleets using bank cards are more vulnerable to fraud
- Where most fleet card fraud originates
- How to measure the total cost of fraud (TCF)
- How managers can identify fraud and minimize reoccurrences

Sources of Fraud Overview

Instances of business fraud are initiated one of two ways: either by someone outside the organization (3rd party), or by an employee.

For most companies, acts of fraud typically originate from outside the company. A study from the Association of Financial Professionals (AFP) found:



- Roughly two-thirds (65%) of companies reported having experienced fraudulent attacks attempted by an outside entity during 2015.[2]
- Fifty percent reported being the target of fraudulent email solicitations, and
- Fifteen percent reported hacks tied to organized crime.

Companies who offer corporate/commercial payment cards seem to be at an even greater risk. The AFP research found that more than three quarters (77%) of commercial card companies were targeted for fraudulent attacks.

Fleets that issue consumer credit cards may unknowingly expose themselves to greater risks.

- Consumer cards lack basic security measures and controls, such as requiring a unique PIN and/or driver ID number
- Little ability to prevent the purchase of specific products and services
- No analytics tools to track and analyze purchasing data for inappropriate purchases
- No ability to create real-time alerts for suspicious activity

Notably, large companies (with revenues of $1B or more) were more likely to experience employee-committed card fraud than smaller companies. Intuitively, this makes some sense. Large companies issue a greater number of cards. More cards in use will generate more transactions, making each transaction more difficult to track and monitor against fraud.

Sources of Fleet Card Fraud

Fleet businesses are susceptible to outside threats, including identity theft and counterfeiting, as well as fraud from employee misuse of their corporate-issued fleet cards.

By necessity, fleet managers must extend some amount of purchasing power to their drivers. At the very least, drivers must have access to a convenient way to purchase fuel for their company vehicles. Additionally, some companies allow drivers to pay for routine maintenance, emergency repairs and other vehicle services using a corporate issued fleet card.

Unfortunately, this flexibility also increases the risk of fraud. Not only is it difficult to fully vet each driver before he or she is granted purchasing authority, the number of transactions that occur each month often makes manual investigation nearly impossible.

External vs. Internal Fleet Card Fraud

Fleet card fraud can originate from both external and internal sources. Some of the more common methods include:

FACT

77%

of companies subjected to an attack were using commercial purchasing cards.

External Fraud

- ***Credit card skimming/cloning***

  "Skimmers" are electronic devices that fraudsters attach to credit card point-of-sale readers. Easily disguised and difficult to detect, skimmers scan the magnetic stripe to gain access to the cardholders credentials. Information is stored and used to create fake "cloned" card accounts.

- ***Lost/stolen "swipe and go" credit cards***

  Most fleet cards require a user to input a unique PIN and/or driver ID to authorize each purchase, but many consumer credit cards are still "swipe and go," allowing anyone to use them.

- ***"Phishing" scams***

  Online fraudsters trick fleet card holders via email or text into revealing their card credentials by posing as a trusted source, such as a vendor partner or company executive. This is also known as "business email compromise," or BEC.

- ***Data breaches***

  Hackers can break into private databases that contain confidential cardholder information to create fraudulent credit card accounts, or sell the information to other criminals.

Internal Fraud

- ***Fleet cards personal use***

  Employees use their cards to purchase fuel or maintenance services on personal vehicles, to purchase non-fuel items or allow others to make purchases with the card.

- ***Misusing company benefits***

  Drivers use merchant loyalty programs for personal benefit. For example, when employees gain access to company-earned discount prices to fuel personal vehicles.

- ***Fuel theft***

  Fraudsters hide "bladder tanks" inside pick-up trucks or vans that are capable of storing a substantial amount of fuel. Typically, the tanks are attached to regular gas tanks and filled during several visits to multiple gas stations. Fraudsters use either their own company-issued cards or counterfeited cards to pay for the stolen gas, which they later resell for profit.

The tell-tale signs of fleet card fraud

- The wrong card is used for the wrong vehicle
- One card is used to fuel multiple vehicles
- Drivers are caught sharing PIN numbers
- Former drivers keep using cards after termination or retirement
- Fuel purchases exceed tank capacity (e.g., 100+ gallons)
- Purchases occur well outside normal operating geography
- Fuel type mismatch: fuel purchased is the wrong grade for a given vehicle
- Too many transactions occur in a given day or week, or outside normal business hours

Frequency of Fleet Card Fraud

Accurate, up-to-date data about incidence of fraud in the fleet card industry is difficult to obtain. In the few industry studies that exist, survey participants often self-report perceptions or anecdotal experience, which can skew results.

The aforementioned AFP study reports that 16% of companies that reported an actual or attempted fraud attack in 2015 were using fleet cards.[3] This percentage holds roughly steady for companies both above and below $1 billion in revenues.

There are several possible explanations for the disparity between commercial and fleet card fraud. For starters, fleet cards are not used universally by all businesses, so they will inherently experience a fewer number of attacks overall.

Fleet Card Fraud Protections

Unlike other corporate/commercial payment cards, fleet cards incorporate several protections against fraud, such as:

Driver Prompts: Drivers must input PIN and ID numbers in order to authorize transactions. Even if a skimmer collects a card's credentials, the counterfeit can't be used without this input as well.

Card Controls: Automatic limits can be set in advance to restrict which products drivers can purchase, in what quantities, where and when.

Suspicious Activity Alerts: Real-time text or email alerts inform managers of when unusual purchases have occurred, or when purchases have occurred outside the usual operational areas/times.

Pump shut-off: Some cards will automatically stop fueling at a pump once a certain quantity or dollar limit has been reached on the card.

Analytics: Sophisticated tracking software allows fleet managers to catch inappropriate purchases that would have otherwise slipped through the cracks.

Employee and Manager Perceptions Differ

A third reason for the disparity between commercial and fleet card fraud may be that fraud among fleet card users is underreported. Perceptions among both fleet managers and drivers, for example, suggest that fleet card fraud may be more common than the numbers suggest.

Recent studies have found that a third of U.S. fleet drivers believe it's acceptable to occasionally use their company vehicle to run a personal errand, while most managers would disagree.

Common Sources of Fleet Card Fraud

When asked to name what they thought were the most common sources of fraud, fleet managers tended to identify deliberate actions drivers took for their personal gain. A plurality of managers (39%) agreed that drivers siphoning fuel occurred very or somewhat frequently, followed by drivers paying for fuel with cash to hide inappropriate purchases (35%).

Drivers, meanwhile, tended to assert fraud was just as much a crime of convenience and/or negligence as an act of intentional misconduct. Drivers said they thought the most common sources of fraud included drivers exploiting loyalty programs for personal use (44%) and negligent driver behavior (32%), in addition to intentional misuse of genuine cards (39%).

CASE STUDY: Fraud in Government Fleets

Some of the only hard numbers about fleet card fraud come from the federal government, which publishes figures about government vehicles.

From 2010 to 2014, the latest years for which data was available, the U.S. General Services Administration reports that government employees committed $2.4 million of fuel fraud using government-issued payment cards. In total, there were 260 cases.[4]

While on their face these numbers seem dramatic, it's worth remembering that government vehicle fleets include over 650,000 vehicles that consume more than $400 million in fuel per year. More than 590,000 fleet cards are in circulation, meaning the rate of fuel fraud over all cards is less than a tenth of a percentage point. Fraud losses accounted for just 0.06% of total fuel spend per year.

The Cost of Successful Fraud Attacks

In 2013, the most recent year for which information was available, the payment card industry estimated fuel-related fraud cost the industry $500 million.[5]

(This figure is not specific to fleet cards, but also includes losses from credit cards, debit cards, etc.)

Steps Fleets Can Take To Reduce the Risk of Fraud

Fleets can implement several policies to deter fraud before it occurs. In the case of both external and internal fraud, the best alternative is often the adoption of a fleet card.

Fleet cards offer powerful security measures, such as driver prompts and card controls, which can help managers rein in unauthorized expenditures. Fleet managers should consider the following actions:

- ***Password-protect*** all company electronics, including laptops, smartphones, and tablets.
- ***Implement an "early warning system"*** for fuel purchases via real-time alerts.
- ***Monitor reports*** for "smoking guns", including purchases that are too frequent, too expensive, or fall outside operational geography.
- ***Regularly audit card use*** to ensure drivers comply with policy.
- ***Deactivate old cards*** with driver/vehicle IDs no longer in use.
- ***Keep spare cards deactivated*** and physically locked in a secure location.

Security training is a valuable tool for teaching drivers and other employees how to recognize and avoid fraud attempts, empowering them to become part of the solution.

Managers should consider security training on:

- How to recognize signs of pump tampering
- Fueling best practices, such as filling up only at stations with surveillance video or at pumps closest to the station
- How to recognize "phishing" scams
- The importance of not sharing cards, passwords and driver prompt information

FACT:

Only 27% of managers reported running security training for drivers.

Conclusions

Fleet cards remain particularly susceptible to fraud committed by both external and internal actors. From the available data, we can draw several conclusions about the motives and incidence rates of fleet card fraud:

- Fleet card fraud is difficult to quantify, but it appears to be lower for fleet cards than for other payment cards.
- Most companies are vulnerable to fraud attacks from external sources, but fleets are also exposed to employee-committed fraud.
- Fleets that rely on consumer credit cards for fuel purchases expose themselves to unnecessary risk of fraud, since fleet cards provide additional security measures that reduce risk.
- Sources of external fraud include skimming, theft, phishing scams, and data breaches.
- Internal sources of fraud include drivers misusing company benefits, fleet cards, and stealing fuel.
- Business' can take several proactive measures to protect against fraud, including the use of fleet cards and better employee security training.

NOTE:

Fleet card fraud is difficult to quantify, but it appears to be lower for fleet cards than for other payment cards.

1. https://www.nilsonreport.com/index.php, March 15, 2017.

2,3. *"2016 AFP Payments Fraud and Control Survey."* March 2016. Association for Financial Professionals, Underwritten by JPM. https://www.pnc.com/content/dam/pnc-com/pdf/corporateandinstitutional/Treasury%20Management/2016_AFP_Payments_Fraud_Report.pdf. This survey included 627 responses from corporations in various sizes and industries. It was conducted January 2016.

4. Nikolewski, Rob. *"Fuel Fraud: Government Employees steal millions from taxpayers at the pump."* Watchdog.org. September 23, 2015. http://watchdog.org/239117/fuel-fraud-taxpayers, March 15, 2017.

5. Sidel, Robin. *"Credit-Card Fraudsters Pump Gas Stations for Profit."* Wall Street Journal. September 3, 2015. http://www.wsj.com/articles/credit-card-fraudsters-pump-gas-stations-for-profit-1441253132, March 15, 2017.

Sponsored by:

WEX Inc.
wexinc.com

CHE 11458