7 Ways to Protect Your Fleet Card from Fraud and Misuse

By Dennis Schiltz, Fleet Fraud Operations Manager at U.S. Bank

Low on fuel, the corporate fleet driver pulled into the nearest gas station and parked at the pump farthest away from the store. Attached to the pump was a gadget adorned with a sign that said, “Please clean your card here before using on pump,” so he swiped his card across it.

Big mistake. The device was not a “cleaner,” but a data skimmer, clandestinely installed by thieves. Instantly, all the information on the fleet card got into the hands of fraudsters, who wasted no time putting it to use.

Sad to say, criminals keep coming up with creative new ways to part us from our money. Fuel cards remain among the most secure forms of payment, but they are still frequent targets of external fraud and internal misuse. That’s why everyone — from fleet card providers to managers to cardholders, must be constantly vigilant and ready to use the tools at their disposal to fight back.

Cardholders themselves are the first line of defense. They can help the cause by following seven simple guidelines when using corporate fleet cards:

1. Store the card in a secure location and never leave it out in the open
2. Keep PIN information in a separate place from the card
3. Do not share the card or PIN with anyone not authorized to use the card
4. Report lost or stolen cards immediately
5. Contact the fleet manager immediately to report any questionable transactions
6. Do not use fuel pumps that do not look right. Go to a different pump or pay inside
7. Watch your card while out of your possession and ensure that it is returned immediately after an in-store transaction is completed

Cardholders' best efforts won't stop all fraud; crooks are too clever and, like it or not, some cardholders themselves are guilty parties (often unwittingly, sometimes not so much). That's where the second line of defense comes in — fleet managers, who play a key role in keeping fraud and misuse at bay through effective monitoring of card data. They get help in that pursuit from fleet card issuers, who are developing increasingly comprehensive tools to spot anomalies. For example, U.S. Bank Voyager Mastercard customers receive real-time alerts and controls that can limit transactions based on number per day, time of day, dollars per week, ZIP code and merchant, among others.

For additional articles, videos and more, visit usbank.com/voyager-mastercard

usbank.com/voyager-mastercard

04-0054-05 (3/23) CAT-13804975

usbank | VOYAGER®