Business Card Fraud

What it is and what you can do

Powered by WEX

Part I: Fraud Prevention Guidelines

The WEX Fraud Department offers the following security guidelines for drivers and fleet managers.

Employees

Keep your Driver ID number secure

- Memorize your Driver ID number number.
- Don't keep your Driver ID number number with your card, or write it on your card.
- Don't give your Driver ID number to a station attendant – enter it yourself.
- Shield the entry of your Driver ID number from any nearby attendants, customers, or passengers.
- Don't enter your Driver ID number as the odometer reading.

Keep your card secure

- Never let the card out of your sight during a transaction. Verify the purchase info, including the amount and date.
- When the card is returned after a purchase, verify that it's the proper card.
- Keep your card where it can't be seen or easily accessed.

Contact your supervisor immediately if:

- Your card is lost or stolen.
- Your Driver ID number is compromised.
- You suspect that fraud or misuse has occurred.

The Chevron and Texaco Business Card Program is administered by WEX Inc. and is not an obligation of Chevron U.S.A. Inc.

CHEVRON, the Chevron Logo, TEXACO, the Texaco Logo and TECHRON are registered trademarks of Chevron Intellectual Property LLC.

CHE_401750_BR_06/2021

Fleet Managers

Register your online account

- If you haven't done so, register your online account. Call the customer service number on the back of your card for assistance.
- After establishing your online account, you can further reduce the possibility of unauthorized card use by setting spending limits. To learn more about these benefits, contact customer service.

Use secure Driver ID numbers

- Make sure all employees have a unique Driver ID number. Don't allow employees to share.
- Avoid easily-guessed Driver ID numbers (e.g., 123456 or 999999).

Verify employee transactions

- Thoroughly review your transaction reporting and perform audit checks against monthly statements.

Establish procedural controls and safeguards

- Perform random and frequent checks to confirm that cards are kept with their assigned vehicles or are in the possession of authorized users.
- Regularly review card and Driver ID number status, and suspend or terminate any no longer in use.
- Provide periodic fraud awareness sessions to your employees.
- Create and share a company policy regarding the misuse of fuel cards by your authorized users, including any legal action that can result.

If an employee is dismissed

- Cancel their Driver ID number immediately.
- Retrieve their card, or cancel any card that may be in their possession.
- Verify that all other cards are in their appropriate location.

Contact your supervisor immediately if:

- Your card is lost or stolen.
- Your Driver ID number is compromised.
- You suspect that fraud or misuse has occurred.

Powered by wex

CHE_401750_BR_06/2021

What should employees look out for when fueling?

- Look for a pump that's well-lit and highly visible to the attendant. Pumps with low visibility are prime targets for skimmers to be installed.
- Check the security label installed on the pump. If it's missing or shows signs of tampering, use another pump or go inside.
- Scan the pump for loose wires, ill-fitting components, pry marks on the panel edges or other suspicious-looking items.
- Visually inspect the pump for any damage to the card reader and key pad. Although most skimming devices are installed inside the terminal, some use overlays on the outside of the pump.
- Keypads should be flush with surrounding surfaces, and card readers should not look overly large for their recesses. Give the reader a quick jiggle to make sure it's attached properly – bluetooth-enabled card readers can be adhered directly over the existing readers.
- Compare the card reader and key pad to those on adjacent pumps to make sure they look the same – do they have the same shape and amount of wear?

Pump security labels, compromised and intact

Bluetooth card readers placed on pump exterior

Key pad overlay example

Powered by wex

CHE_401750_BR_06/2021

Part II: Security FAQ

Fraud and Abuse

What is 'skimming'?

Skimming is when the information on a payment card is captured and used to create a counterfeit card (also known as "white plastic"). The counterfeit card is then used to make illegal purchases. Criminals can install skimming devices on the interior or exterior of fuel dispensers.

How does WEX define 'fraud' vs 'abuse'?

- **Fraud** is third-party criminal activity for financial gain; a customer had possession of their card and an unknown individual accessed their account.
- **Abuse** is when a customer's employee or other authorized user uses the business card for unauthorized purchases. In this case, the customer should follow internal procedures for investigating and restitution.

What fraud protections do business cards provide?

- **Card controls.** Automatic limits can be set in advance to restrict which products can be purchased, in what quantities, and when.
- **Pump shut-off.** Cards can automatically stop fueling at the pump when a certain quantity or dollar limit has been reached.
- **Analytics.** Real-time and scheduled reports allow fleet managers to identify inappropriate purchases that would have otherwise slipped through the cracks.

Are instances of fraud increasing?

Fraud, specifically pay-at-the-pump card-skimming scams, has reached epidemic levels in the US. Task forces have been formed in the hotspot areas, including Texas and Florida. WEX is collaborating with these agencies to help build cases and ultimately execute arrest warrants.

Who is financially responsible when fraud occurs?

There are four basic categories of fraud:

- **Lost or stolen cards.** The customer is liable for any damages before reporting these cards to WEX.
- **White plastic (skimming).** The customer is not liable for charges if the claim investigation reveals the transactions in question are the result of skimming by an unknown third party
- **Collusion.** If an investigation reveals that a customer employee and fueling station were colluding to steal funds or fuel from the account, there may be a liability split. The station would be charged back for half of the losses and the customer would be liable for the remainder.
- **Driver abuse.** Customers are liable for employee card abuse. As stated above, the customer's internal procedures should be leveraged for investigation and restitution.

Powered by WEX

CHE_401750_BR_06/2021

Our Fraud Detection Systems

What systems does WEX use to detect fraud?

WEX leverages a fraud detection system based on neural models (machine learning). We also have a data analytics engine that provides instant feedback on which detection rules are most effective and which ones need to be changed or retired. Our fraud detection system looks at authorizations and transactions at the account, card and driver level to learn behavior and alert us to any deviations from prior purchasing behavior.

If fraud is suspected at a station, why won't WEX share their name and address?

When cards are compromised, there are two things to consider:

- **Where the card was skimmed**
  We DON'T release this info, because investigations are most likely underway. The stations are also victims in this situation — an unauthorized third party has broken into the pumps and installed a skimming device. In most cases, once the device is removed, there is no longer an issue.
- **Where the compromised card was used**
  We DO release this info, so we can validate that the card in question was not actually at the station in question.

Additional Info

What else can I do to prevent fraud or abuse in my program?

- Password-protect all company electronics, including laptops, smartphones and tablets.
- Monitor reports including purchases that are too frequent, too expensive, or fall outside operation geography.
- Regularly audit card use to ensure that employees are complying with policy.
- Deactivate old cards with Driver or vehicle ID numbers no longer in use.

What are the telltale signs of business card abuse?

- The wrong card is used for a particular vehicle.
- One card is used to fuel multiple vehicles.
- Drivers are caught sharing Driver ID numbers.
- Former drivers keep using cards after termination or retirement.
- Fuel purchases exceed the tank capacity.
- Purchases occur well outside normal operating geography.
- The 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.

Powered by wex

CHE_401750_BR_06/2021