Help prevent credit card fraud in your trucking business

wex™

1764441317 (1/25)

Fraud is on the rise and comes in many forms. As Alessandro Mascellino reports in a May 2024 article for Infosecurity, there has been a 341% rise in "malicious phishing links, business email compromise (BEC), QR code and attachment-based threats in the past six months."

Over the last several years, fraud has become increasingly difficult to detect. For those of us who've been in the business for a number of years, when we think of phishing, we think of something terribly written and obvious in its nefarious origins. Due to AI, what used to be transparent and detectable signs of fraud are no longer so apparent. Bad actors have become more sophisticated and their content is much more believable as a result.

Fraud is on the rise: What to do about it

The question now becomes: What do you do about the rise in fraud, and how can you protect your business from this insidious, predatorial behavior?

Most fraudsters focus on accessing cash, credit, or goods that they can resell for a profit, which can harm your business and impact your bottom line. In this white paper, we review the most common forms of credit card fraud and how to prevent them from impacting your business.

What are the most common forms of fraud?

Transaction fraud

Transaction fraud describes a couple of different types of fraud, including:

- **Fraud with a skimming device**
  A common form of fuel card fraud happens when someone illegally obtains card data through a skimming device. Criminals install hidden devices on fuel pumps or point-of-sale terminals to capture the user's credit card information (like card number and PIN) when they swipe. They "skim" the data off the card without a driver's knowledge, and then use that information to make fraudulent purchases.
- **Lost/stolen cards**
  Thieves find a lost card or steal a company card and use the card for illegal purchases.

First-party fraud

First-party fraud is the easiest to detect and the most difficult to prosecute. Anytime an authorized representative makes a transaction using their own identity to commit fraud, it's called first-party fraud. This fraud is particularly onerous because the user perpetrating the fraud is authorized to authenticate the transaction.

Here are a few examples of how first-party fraud could look in practice:

- An individual applies for a loan or a credit card with their real identity but with no intention of paying back that debt. For example, say a business owner finds themselves in a tight financial situation. To bail themselves out, they knowingly draw credit they won't be able to or don't plan to repay.
- When a business opens a fleet card account, they give each driver a fuel card the driver is authorized to use. First-party fraud occurs when one of those drivers uses their card to purchase fuel for a personal vehicle or to sell to an outside party for profit.
- When an employee uses their company card to fuel their friends' vehicles during a single transaction.

First-party fraud experiences upticks during economic downturns where businesses or individuals can unexpectedly find themselves strapped and unable to make ends meet.

Account takeover

Account takeover is a type of fraud involving a cybercriminal accessing a user's online accounts. The criminal obtains login credentials through fraudulent means, using them to illegally access another person's cash, products, and personal account information. If there is one app or website the victim has access to that is improperly secured, the floodgates open for the cybercriminal to wend their way through connecting paths to get to other accounts and do a clean sweep of assets.

Account takeover has tentacles that reach into layer after layer of accounts causing all kinds of mayhem for the victim. This type of fraud is difficult to counteract and has far-reaching implications.

Application fraud

Another common form of fraud is application fraud. This is when a fraudster applies for credit using stolen or inaccurate information.

Application fraud and first-party fraud overlap. This is because application fraud often involves legitimate consumers using their own identity to commit fraud. These types of fraud are the hardest to detect because they involve the use of a true, authenticated identity.

How do I protect my fleet fuel card from fraud and the negative impact it would have on my trucking business?

As phishing and other types of credit card fraud increase in sophistication, here are some actions to take to help prevent damage to your business:

Update the product purchase limits on your fleet fuel card

- Limit the number of times a product or service can be purchased and/or the number of transactions your fuel card(s) can perform in a given day, week, or month.

Implement time restrictions

- Restrict fuel card usage to specific days and times. This increases control and visibility, helping prevent misuse.

Require real-time, trip-number validation

- Adding a trip number prompt to your fleet fuel cards – and updating this number as drivers are dispatched on new trips – is another way to prevent fraudulent activity.

Activate site restrictions

- Lock down your fueling network to only necessary merchants.

Require exact match prompting

- Requiring drivers to enter specific values at the point of sale in order to perform a transaction can help mitigate fraud. WEX's Dynamic Prompt requires two-factor authentication at the pump. This exact match prompting can help protect your accounts from fraud. See more below on Dynamic Prompt.

Appropriately manage card status

- Clean up unused and idle cards by updating their status to "hold" or "inactive." This will prevent bad actors from reactivating idle cards.

Implement SecureFuel

- **Set up SecureFuel on your account for added security**. See below for more information.

Require regular employee training

- Regularly educate your employees on the most common phishing scams and social engineering tactics. Empower your employees to say "no" to any requests that feel out-of-the-ordinary or give them pause. Provide mandatory, annual fraud training.

Among these simple best practices, perhaps the most important thing you can do is educate your employees on how to be vigilant and give them the agency to decide on the fly what might be fraudulent and what to do to prevent further action from fraudsters.

What companies and individuals can do to stave off social engineering fraud

Your biggest defense against fraud is your people. According to the **2024 Association of Fraud Examiners (ACFE) Report to the Nations**, the median annual fraud loss for businesses is $145,000. Fraud impacts an estimated 5% of revenues annually. If you build a culture of education, trust, and agency, your staff will have the power to ecognize and take appropriate steps against fraud.

Our research shows that newer employees are better than veteran employees at fraud prevention and identifying socially engineered communications. This is likely due to fraud prevention training during onboarding that's still fresh in their minds. Veteran employees either never received such training or could benefit from a refresher course. The best way to solve this is to make annual, mandatory fraud training part of your business plan and an expectation and priority for your staff. There is great value in constantly retraining and providing fresh information to your entire organization.

Teach your staff to say "no" to fraudsters

Additionally, what we've seen in our research is that the most secure environments empower staff to say "no" to fraudsters. Cultures where staff are most vulnerable perpetuate a fear that saying "no" to a perpetrator will mean job loss or other consequences. Fraudsters are manipulative and use menacing tactics to convert your staff, sometimes even threatening that they will lose their jobs if they don't do what they are told. This forces your staff to take actions that allow criminals to infiltrate your systems. If you empower your staff to be cautious and not easily manipulated, you can avoid this kind of fraud impacting your business.

Train employees on fraud prevention

Here are some basic rules to teach your staff to avoid harmful phishing schemes:

- Never click links you don't know.
- Never respond to emails when you don't know the sender.
- Never respond to an unsolicited email asking for account information.
- Do not provide sensitive information over the phone or email.
- With more sophisticated forms of fraud, the domain or sending email is what becomes the tell. Train your employees to ask themselves, "Does this email address make sense?" and avoid clicking on attachments or links sent from an unfamiliar email address.
- Give your employees the power to say, "I need to authenticate this before I can go any further." And provide the tools to jump-start that authentication.
- Make sure your employees understand that they will never get fired for asking a caller or emailer these kinds of probing questions, nor will they get fired for saying "no" to someone asking for account information.

Fraud: What to be on the lookout for and what to do if you feel you've been compromised

A currently surging fraud trend involves receiving AI-generated phishing emails from illegitimate sources. These emails – circulated globally and crafted in a more sophisticated language – are harder to detect. It's important to remind your employees who handle these emails that WEX will never ask for login credentials to your fuel card account over email. If one of your staff inadvertently responds to a phishing email and provides credentials to a cybercriminal, they should immediately call WEX's customer service number (printed on the back of all WEX fleet fuel cards). Alert us that your business has been compromised, and we will take the necessary steps to mitigate any attempts at fraud on your account.

Dynamic Prompt with two-factor authentication technology increases fuel card security and savings

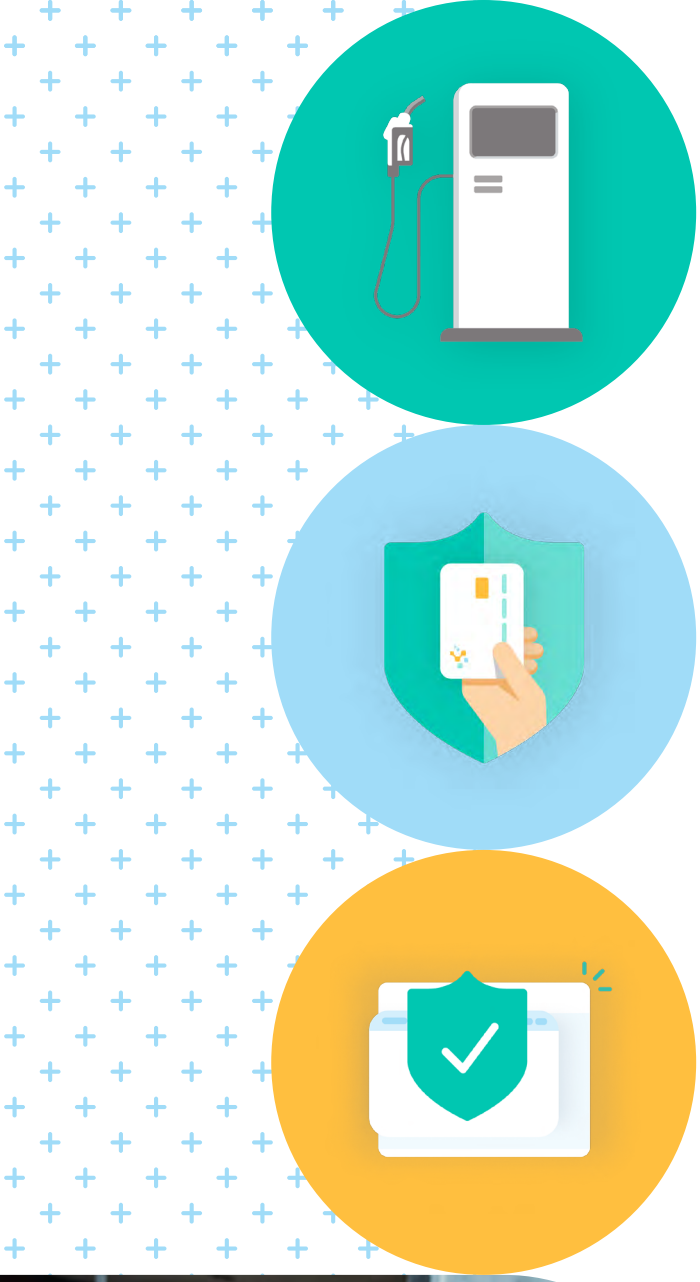
WEX has designed a security feature – Dynamic Prompt – that minimizes the threat of fraudulent activity with two-factor authentication, creating an additional barrier to prevent skimmers from being successful. This security feature helps you avoid disruption to your business and keeps your drivers moving.

Download our Dynamic Prompt infographic and share it with your drivers.

Log into eManager to learn more about Dynamic Prompt two-factor authentication from WEX.

Technology that builds ironclad fleet card security

- **Dynamic Prompt helps prevent card skimming with two-factor authentication**
- **SecureFuel technology provides protection and control for over-the-road fleets**



Add fuel card security features with SecureFuel

Did you know you can add SecureFuel technology to many WEX-issued trucking fleet cards? This technology provides greater fleet card control, gives fleet managers sophisticated data reporting and telematics features, catches fraudulent behavior, and helps prevent misuse.

SecureFuel technology delivers innovation to the fleet card industry

SecureFuel technology – which doesn't require any hardware – integrates with the unit from a truck's built-in telematics data to monitor fueling transactions in real time, creating more ways to keep an eye on your vehicles. As credit card fraud continues to plague businesses and becomes more sophisticated, this technology can be valuable to your business.

When a driver attempts to purchase fuel with a fleet card, SecureFuel technology checks the truck's location and tank level before securely authorizing the purchase. By combining telematics with fleet card transaction data, SecureFuel technology identifies any unauthorized purchases or misuse, and companies can choose to be notified immediately of the incident or even decline the transaction.

SecureFuel technology provides ECM reconciliation and protects skimmed cards from being used

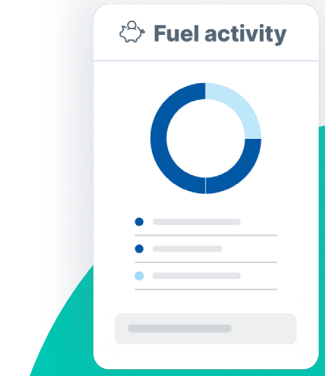
By combining truck telematics with fleet card transaction data to pinpoint suspicious transactions in real time – and by providing a report on the vehicle's proximity and tank level after fuel purchases – SecureFuel can quickly find purchase irregularities and trigger an alert to you or your fleet manager. SecureFuel is one of the industry's only solutions that uses the truck's engine control module (ECM) with no additional hardware needed. SecureFuel technology works at more than 16,000 truck stops across the United States.

Learn more about SecureFuel from WEX.

General security practices for fleet card managers to prevent fraud on your WEX account

The following suggestions and procedures can also help protect your business from fraud:

- **Periodically review eManager and your personnel's purchasing limits.** WEX can supply this list very quickly upon request.
- **Keep WEX notified about attrition.** Immediately notify WEX when a person with access to eManager leaves the company. Adding WEX to the procedures for employee removals will serve as a good reminder to make sure WEX's authorized list of personnel is always up to date.
- **Stay on top of "Reject" reports.** Review rejects periodically to understand what transactions were blocked. This may indicate malicious/ unauthorized attempts on your card by drivers.
- **Track MoneyCode transactions.** Review the checks and balances when a MoneyCode is created for one of your drivers.
- **Keep drivers informed and vigilant.** Remind your drivers not to provide their PINs to anyone. Just like with a personal credit/debit card, your PIN protects your account. This information should never be shared with anyone.
- **Password protection is a priority.** Do not share your eManager username or password with anyone, for any reason.



Want to learn more about more effectively managing your trucking fleet? Explore additional WEX over-the-road articles and insights here:

- Fuel card FAQs
- Safety tips
- Fraud prevention
- Tax prep

Don't yet have a WEX Over-the-Road fuel card for your trucking business? All fleet cards are not the same, and different types of fuel cards suit the needs of different kinds and sizes of businesses. View WEX's **fleet card comparison chart** to see which fleet fuel card is right for you.

Apply for a fleet card today!

Resources:
Infosecurity Magazine
National Association of Fraud Examiners