Fuel card fraud – A breakdown of current trends (Part 2)

In the second part of this article, Carsten Bettermann, CEO of UTA and Mark Goldspink, CEO of The ai Corporation, look at trends and different types of fraud in the fuel cards ecosystem in Europe.

There are many types of fraud that road transportation and fleet operators need to be aware of. By far the most common type is skimming and copy card fraud, which together account for most fraud during the past three years. According to ai, 97% of cases in Italy were related to skimming in 2019.

Skimming and copy card fraud

Skimming and copy card fraud is where card data is stolen during a point-of-sale transaction by the cashier or via the card reader. Sometimes it's committed with the cardholder in exchange for money, often at driver rest areas. UTA estimates colluding cardholders are paid approximately €1,000 per card.

Stolen data is used to create a copied card, often designed to mimic a real (maybe expired) fuel card to avoid suspicion in the event of being stopped and searched by the police. Increasingly, criminals are using technologies, such as Bluetooth and WiFi, to transmit card data from skimming devices that have been inserted into card readers.

Alternatively, criminals fit entrapment devices into card readers, which prevent cards from being returned to the cardholder. These are used in conjunction with a small camera to capture the PIN as it is entered. Once the cardholder returns to their vehicle, the criminal removes the device and card.

Once copied, cards are typically misused at unmanned stations or outside payment terminals at manned stations at a different location to where they were skimmed, often at night or at the weekend.

More traditional forms of copy card fraud include 'shoulder surfing' – in which criminals watch as a user enters their PIN; or breaking into a parked vehicle, typically at a rest area or dedicated truck parking location, to copy card data. Fraudsters know that truck drivers often leave sticky notes in their cabs with card and PIN details. Once they locate and copy the information, they often exit the vehicle without a trace, leaving drivers unaware that their cards have been compromised.

Chip & PIN cards offer some protection against skimming but are not immune due to the current fallback to magstripe when the chip is damaged or unreadable. Fraudsters will simply damage the chip by scratching it and overlaying it with a fake sticker so that it cannot be used, or by simply smashing the chip out with a hammer.

In addition to skimming and copy card fraud, other types of card fraud include:

Lost and stolen card fraud

When criminals steal cards and, where possible, PINs. Even without a PIN, stolen cards may be used fraudulently at networks that do not require a PIN such as online web purchases. Most fraud relates to purchases on cards prior to them being discovered or reported as lost or stolen or purchases on cards due to delays in blacklisting or restricted blacklist quotas.

Site collusion

This is where drivers collude with site staff to transact for fuel when refuelling has not taken place or to charge more for the fuel. The value is often exchanged for cash or goods such as cigarettes. This is sometimes referred to as ‘dieselization’. Knowledge of sites open to collusion is often passed between drivers.

Abuse of a genuine card by the cardholder (driver fraud)

When a card is used for purposes other than for which it has been authorised. For example, purchasing fuel for another vehicle or driver in exchange for cash; purchasing fuel with a valid card but siphoning the fuel from the tank; using a ‘bladder tank’ hidden inside the vehicle; damaging a chip or magstripe to override purchase controls or to justify paying for fuel with cash to hide the purchase of unauthorised goods; or drivers using details of cards from previous companies, etc.

Driver fraud is particularly hard to identify because it tends to follow the “normal” buying behaviour for the driver.

Internal fraud

Here, employees or contractors act alone or in collusion with external parties (either willingly or due to coercion or bribery) to steal data, information, or materials of a commercially sensitive nature or which could be used to compromise a company’s operations or security.

Mail non-receipt/intercept fraud

This involves the interception of cards and/or PINs at a customer’s address, at a mail sorting hub or within the postal distribution system. Compromised cards are copied, re-posted, and delivered to the customer. Customers most at risk are businesses with communal letterboxes or those that do not get mail redirected when they change address. Similarly, cards and PINs are known to have been intercepted in mail sorting hubs at airports and elsewhere.

Identity and application fraud

Criminals can impersonate or take over a genuine business to open an account using fake or stolen documents. If a fake application is successful, fraudsters are issued with cards and access to other services and are invoiced with several days before payment is due, giving them ample time to commit fraud. Non-payment of an invoice is often the reason the fraud is discovered.

Card-not-present fraud

This involves the theft of card details used to make a purchase online, leaving the genuine cardholder unaware until they check their statement. Criminals obtain fuel card numbers using special software that generates valid card numbers, or via skimming and data breaches, and then sell the cards to drivers who use them at toll networks. Criminals (typically a former employee) will access online portals to order ferry tickets, Eurovignettes and tolls using the card details of their previous company for the vehicles of another (typically for their current employer or possibly an owner-driver with whom they are colluding).

Vehicle cloning

In this scenario, the registration number of a genuine vehicle is copied and used for another vehicle of the same make and model for the purpose of avoiding fuel, toll, and parking payments, congestion charges, and more.

Strategies for fuel card fraud prevention

So, what steps can businesses take to reduce the risk of card fraud and thwart the ever-evolving efforts of criminals? For one, card issuers, fleet managers, partners, and card users must work together to achieve the highest levels of security.

As fuel card fraud has developed into a Europe-wide threat driven by international gangs, detection and prosecution require the cooperation of international institutions and authorities. Two major authorities in this field are the Fuel Industry Card Fraud Investigation Bureau (FICFIB), a group of card issuers, fuel retailers and independent service station operators that share intelligence on trends, vulnerabilities and developing threats; and Europol, which shares information on cross-border incidents with local police forces to assist customer incidents and investigations. Close cooperation with institutions gives card providers the international clout they need for successful action in the event of an incident.

In addition to cooperation with authorities and institutions, it is crucial for card providers to set up, continuously monitor – and if necessary – optimise their own products, services, and processes. This begins with the design of products and services such as real-time transaction notifications and includes the regular qualification of customer service and IT processes to ensure criminal activity can be countered as quickly as possible.

Finally, communication is a crucial component of card security. Communication processes with

authorities, partners and customers must be fast and focussed. In the event of fraud, rapid communication with anyone affected is critical. Furthermore, it is important to raise awareness among customers and partners about the dangers of fuel card fraud, and to offer them support in its prevention.

*By **Carsten Bettermann**, CEO of UNION TANK Eckstein GmbH & Co. KG (UTA) and **Mark Goldspink**, CEO of The ai Corporation (ai). Both companies are* working together to prevent and detect fraud. More insights into the complex field of fuel card fraud and the prevention measures that should be taken can be found here.