The changing nature of fuel card fraud in Europe (Part 1)

In the first part of this article, Carsten Bettermann, CEO of UTA and Mark Goldspink, CEO of The ai Corporation, analyze the growing risk of fraud in the fuel cards ecosystem in Europe.

Fuel cards and contactless toll settlement devices have become critical operational tools for commercial road transport operators across Europe. Given the number of tolled motorways, bridges and tunnels in the region, and drivers' reliance on refuelling stations to help them reach Europe-wide destinations in a safe and timely manner, technology is now being used to ensure supply chains remain open and efficient.

Given the convenience fuel cards and contactless toll settlement devices provide to drivers, the visibility and control they deliver to employers, and the worldwide migration towards cashless settlement methods, it's no wonder their use is on the rise. In many cases both technologies have become critical expense management tools for many in the road haulage sector. Allied Market Research estimates that the value of the global fuel card market, recorded at $672 billion in 2019, will almost double to $1.2 trillion by 2027.

However, like all payment channels, especially those that are growing, like fuel cards, there is a growing risk of fraud. Indeed, fraud incidents have significantly risen over the years, as criminals employ increasingly sophisticated techniques to infiltrate the security of cards and settlement devices. Fraud has become more common during the COVID-19 pandemic, as more transactions are made online and the value of individual transactions increase. Fraud cases were higher in 2020 than they were in 2019, with much of the increase seen in toll, tunnel, and bridge-related fraud.

As the purchase of fuel accounts for up to 30% of a fleet's running costs, any manipulation, misuse, or theft of fuel cards could have a serious impact on profitability and the potential for losses of tens of thousands of euros in days.

Card fraud is evolving and spreading across Europe

From individual criminals toward organised and international crime groups; from skimming of a single card towards data breach attacks; and from criminals working across the entire fraud lifecycle to fraudsters specialising in part of that value chain and selling that value on to the next level.

At the same time fraudsters are becoming more sophisticated through:

- Device spoofing
- Location manipulation
- Threats and bots
- Business fraud
- Assuming fraudulent digital identities
- Masquerading as customers
- Offering fraud-as-a-service (FaaS) often via the dark web – conducted either by global crime syndicates or by lone fraudsters

In today's digital age, fraud techniques are growing more sophisticated by the day. In the past, criminals typically copied a single fuel card, but today they often produce multiple versions and distribute them simultaneously to fellow conspirators across different countries for maximum financial gain. To pull off such a feat, criminals must be organised. And indeed, many are – often part of larger cross-country gangs involved in drug dealing, people trafficking, gun running, or worse.

Organised gangs are rife throughout Europe(1), and many have adopted a geographic focus to their fraud efforts. Analysis indicates that one gang focuses on motorway service stations at major east-west or north-south junctions in France, while another concentrates on the southern border of the Netherlands where it adjoins Belgium and Germany.

Latest findings indicate significantly increased criminal activities along the route from Bordeaux to Irun in Spain, at the Italian east coast and on routes leading from Italy to Slovenia. Also, the French border with Germany and Switzerland showed a rise in card fraud incidents over the last months.

Other gangs target drivers based on their country of origin – countries in which they may have co-conspirators who help perpetrate the fraud. For example, it is suspected that gangs in France and the Netherlands may have links to Eastern Europe and may be targeting drivers from that region. It is certainly the case that most Eurovignettes purchased fraudulently online are for vehicles belonging to companies based in Eastern Europe.

In general, fraud is mirroring the success of transport companies based in Eastern Europe moving goods west and south through Italy and France through to Spain and north to Scandinavia and back. France has become a fraud hot spot due to its status as a transport hub and because of its prevalence of unmanned fuel stations.

Most skimming takes place at unmanned stations to the north and east of Paris and in the main transport hubs around Lyon and Grenoble. Further south, Perpignan saw a spike in crime in the first quarter of 2021. Fuel stations and rest areas along the French/Spanish border and in the Venlo border area of the Netherlands are the main locations for vehicle break-ins and the misuse of copied cards.

There is no doubt that monitoring fraud event rates and geographic distribution can be very helpful in preventing fraud and being able to react quickly if it occurs. However, it is imperative that we

continue to focus on enhancing technology and preventative measures within the fleet card ecosystem. To do this effectively, we need to know where and how individuals learn the techniques for committing fraud and the rationalization of their criminal activity. We also need to safeguard against creating process gaps, where individuals may become tempted to commit fraud by adopting a constant lesson's learnt approach, which is why communication and collaboration as fraud prevention agents is key. Standing still is not an option.

(1) Source Europol: A single mass copy attack in the Netherlands exploiting velocity loopholes took $800,000 within weeks. In Italy, an attack within on-site velocity limits took $3.2m in less than two months. In 2018, Europol broke up a Spanish crime group using counterfeit fuel cards within Spanish and French toll networks: 24 arrests were made, 600 vehicle registrations were compromised, 11 card factories were dismantled,15,000 counterfeit cards were seized, and a loss of €500,000 was identified.

Part 2 of this article will follow.

*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.