Mind the Trap

Fuel Card Fraud and How to Prevent It

Be Smart:
Guard Your Card

Contents

01 Fuel card fraud in Europe

Insights and strategies to ensure card and transaction security

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.

Given the convenience fuel cards and contactless toll settlement devices provide to drivers, the visibility and control they deliver to employers, and the worldwide gravitation toward cashless settlement methods, it's no wonder their use is on the rise. 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, the downside of these cards' popularity is the 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.

The issue has become more acute during the COVID-19 pandemic as more transactions are made online. Fraud cases were higher in 2020 than they were in 2019, with much of the increase seen in toll, tunnel and bridge-related fraud.

Given the level of consumption and the price of fuel as well as the scale of many modern fleets, fuel is one of the highest costs any transport operator must bear and can account for up to 30% of a fleet's running costs. Thus, 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.

01

Fraud examples from recent years:

- In 2015, German Federal Criminal Police Office investigators apprehended a gang of fuel card counterfeiters who reportedly caused €3.5m worth of damage across Europe by card skimming.
- In a case from 2017, Austrian authorities, together with Bavarian and Italian police, investigated eight suspects alleged to have stolen 288 toll and fuel cards from parked trucks and caused damage amounting to €1m.
- In 2020 in Germany, a truck driver with two manipulated fuel cards stole diesel worth approximately €100,000.

Against this backdrop, it's no wonder that fraud protection and security is an important factor for customers when it comes to choosing a fuel card service provider.[1]

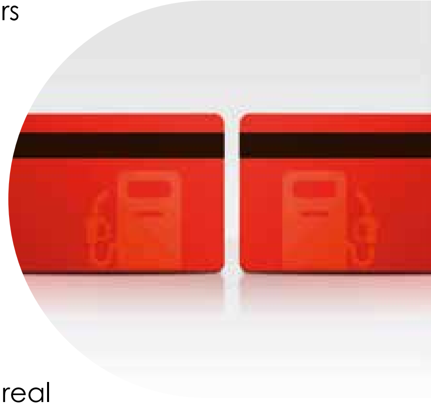
The aim of this white paper is to give fleet managers and professional drivers insight into the issue of fuel card fraud to raise awareness of security risks and preventive measures. UTA's Fraud and Card Security Team has identified the modus operandi and regional fraud 'hot spots' in Europe through which different types of card fraud is committed.

Incidents of fraud are on the rise.

[1] Source: Datamonitor

02 A typology of fuel card fraud

Skimming and copy card fraud



There are many types of fraud that road transportation and fleet operators should be aware of. By far the most common type is skimming and copy card fraud, which together account for the majority of all fraud during the past three years.[2]

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 mimick 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 sometimes 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.

Skimming and copying cards are the most common types of fraud.

[2] According to AI Corp, 97% of cases in Italy were related to skimming in 2019

02 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.

02

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 sometimes 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 a number of 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.

02 The profile of a fraudster

The following characteristics are typical of fraudsters[3]:

69%

are between **36-55** years old

79%

are **male**
(but the proportion of women is rising)

62%

are likely to have **colluded** with others

65%

are employees committing fraudulent acts **against their own employer**

35%

are members of **senior management**
(including board members)

38%

worked at their company for at least **six years** before committing fraud

Large-scale fraud usually involves senior members of management who override process-level controls through their high level of authority.

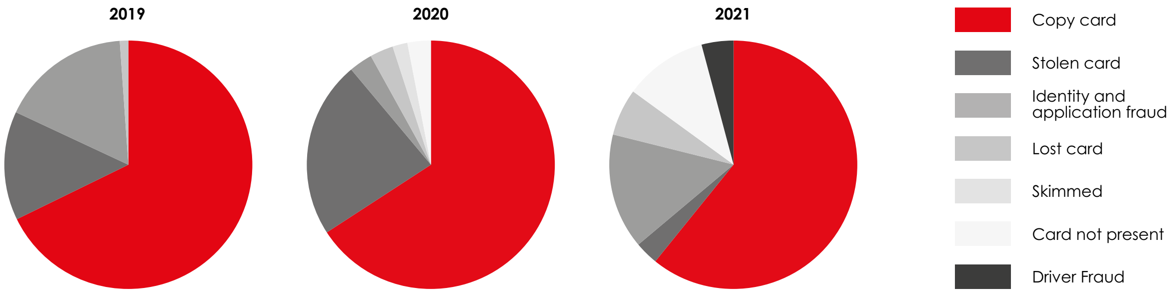
In addition, fraudsters typically:

- Do not take holidays
- Are secretive about business processes
- Are resistant to supervision
- Have poor inter-personal skills
- Have good technical abilities
- Work late
- Are prone to substance/alcohol abuse
- Are prone to relationship discord

[3] Source: KPMG Global Profiles of the Fraudster, 2016

02 Examples of the evolution of fraud in Europe 2019-2021

Fraud type contribution to total losses per year



Because fraud threats are constantly changing, regular risk assessments and the continual evolution of prevention and detection methods are vital for maintaining high levels of security.

Card fraud is evolving:

- From individual criminals toward organised and international crime groups
- From skimming of a single card towards data breach attacks
- 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

Fraudsters are becoming more sophisticated through:

- Device spoofing
- Location manipulation
- Threats and bots
- 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

03 The regionality of card fraud

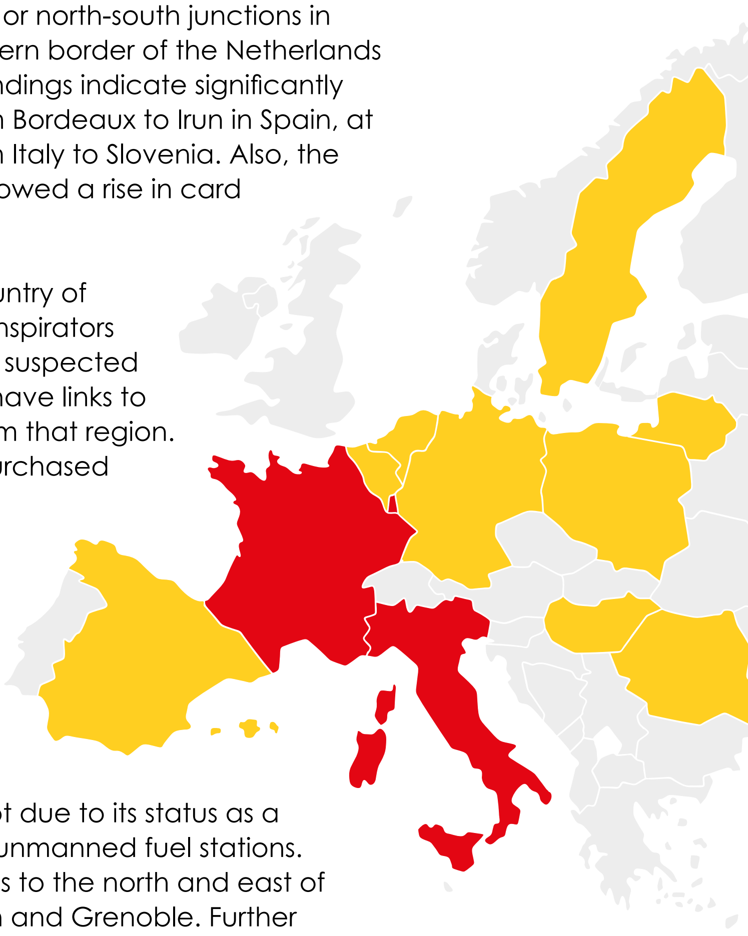
Hot spots and regional trends in Europe

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[4], 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.

Still 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.



Fraud hot spots
2019 - 2021

France in particular 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.

Monitoring fraud event rates and geographic distribution is helpful in preventing fraud and being able to react quickly if it occurs.

[4] 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.

04 Strategies for fuel card fraud prevention

What can be done to reduce the risk of card fraud and thwart the everevolving efforts of criminals? For one, card issuers, fleet managers, partners and card users must work together to achieve the highest levels of security.

4.1 Measures for fuel card providers

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 transaction notifications and includes the regular qualification of customer service and IT processes to ensure real-time 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.

04

4.2 UTA's approach to card fraud prevention

As a mobility service provider, fuel and service cards are a cornerstone of UTA's product and service portfolio. Consequently, card and transaction security is a priority.

At the centre of UTA's anti-fraud efforts is its dedicated Fraud and Card Security Team covering responsibilities such as:

- Real time transaction notifications enable customers to intervene immediately
- Alert customers by phone if suspicious events are detected
- Develop and implement strategies and processes for the effective detection, prevention and mitigation of fraud
- Recommend techniques for limiting the risk of fraud
- Collaborate with lawyers, law enforcement agents, the FICFIB, and others to develop and execute plans for the resolution of fraud cases
- Develop and monitor reports and information useful in apprehending fraudsters
- Conduct interviews with victims and suspects to obtain information regarding the nature of an attack and determine their potential involvement

> *"Through our products, services and processes, we're committed to protecting our customers against current and emerging forms of fraud."*
>
> Carsten Bettermann,
> CEO of UTA

Card and transaction security are key success factors in the mobility services sector.

04

Leveraging industry intelligence

One reason for UTA's high fraud detection rate is its deep subject matter expertise accrued through years of collaboration with leading security organisations, industry bodies and third-party experts.

Where UTA does not have in-house expertise, it partners with specialists – for example, in areas such as cyber forensics, emerging threats to payment cards and banking products, trawling the web, or in-depth crime investigations. As an example, for algorithm-based automated and optimized fraud detection UTA cooperates with The ai Corporation Ltd, a specialist for artificial intelligence-driven systems for payment security and transaction monitoring. Also, UTA is a member of the FICFIB, coordinates with Europol, and is an active member of industry bodies which set common standards for the secure exchange of data between acceptance networks and card issuers.

Furthermore, UTA works with service station operators in 40 European countries to ensure they have security in place on their forecourts, such as CCTV or IP cameras, defences against the installation of skimming devices and online transaction authorisation capabilities.

As part of the global Edenred group, UTA benefits from expertise in areas such as compliance, data privacy and IT security. Edenred's longstanding Fraud Forum spans all lines of its business in more than 50 countries, sharing insights and best practice on topics ranging from fraud types to litigation.

> “*Artificial intelligence and machine learning are indispensable tools today to effectively prevent fuel card fraud and quickly detect fraud cases. In our cooperation with UTA, we combine the state of the art technical systems (aiAutoPilotML) and the know-how of our fuel card experts with the comprehensive expertise that UTA brings to the table in the area of prevention and detection of fuel card fraud. Through this bundling of technology, experience and expert knowledge, we achieve a very high impact and success rate in preventing and combating fuel card fraud.*”
>
> Dr. Mark Goldspink,
> CEO of The ai Corporation Ltd

Combining in-house expertise with specialist partners to achieve optimum results.

04 Taking a proactive, preventative stance

Alongside its subject matter expertise, UTA takes a preventative, 'security by design' approach to ensure its platforms and products are built from the ground up for maximum security. Furthermore, the company invests significantly in R&D in areas such as data analytics, artificial intelligence and machine learning to help its Fraud and Card Security Team detect an ever-expanding range of fraud types faster than ever before.

For example, to combat the mass counterfeiting of fuel and toll cards, UTA has implemented geographical plausibility checks that track the time and distance between locations to see if it's physically possible for a transaction to be legitimate or not. When issues are identified, cards are blocked immediately and customers are notified.

Having such granular visibility of the European fraud landscape enables UTA's Fraud and Card Security Team to act to minimise customer risk, enlist the support of Europol and other security authorities if necessary, and share intelligence across the FICFIB.

> “ *We are currently developing our new digital fuelcard. This advanced solution combines UTA's expertise in transaction security and fraud prevention with our parent company Edenred's deep knowledge in payment services.“*
>
> Carsten Bettermann,
> CEO of UTA

Digital fuel cards - faster, more convenient and more secure

Contactless digital settlement procedures are on the rise - a trend accelerated by the COVID-19 pandemic. Digital fuel card applications on a smartphone not only allow easier fuel purchases at the pump, but ensure faster and more efficient processes, from logging in and registering in the system to managing one's own data and bookings. Another advantage is the additional layer of transaction security such digital cards provide over physical fuel cards.

04 Minimising customer risk

To reduce the risk of card fraud to customers, UTA has implemented a range of security features and services. They include 24/7 card blocking via the UTA online portal, PIN numbers for all cards, enabling customers to set their own card spending limits, providing control over where and when products can be purchased, and transparent invoicing and reporting. Customers can cap the amount that cards can buy as well as limit the days of the week and times of the day that they can be used.

UTA's Transaction Notification service alerts customers in real time when transactions are made on UTA fuel cards, enabling them to intervene if they spot anything suspicious. The service can be tailored to a customer's requirements – for example, filters can be set to send notifications via text or email, set a minimum value per transaction for any alert, or set country-specific date or time restrictions.

Finally, UTA supports customers who fall victim to fraud by contacting the supplier – for example, the fuel station operator – to request that they save any video or CCTV footage for police investigations. Where appropriate, the UTA Fraud and Card Security Team will liaise with the police to provide information which may be used as evidence or to identify other potential victims.

A track record of success

In summary, UTA strives to anticipate, pinpoint and neutralise criminal activity before it can affect customers – a stance in which it enjoys a high rate of success. The company identifies nearly 90% of incidents before they are spotted by customers. Two years ago, this figure was 63%, underscoring the effectiveness of the company's efforts. As well as spotting more incidents of fraud, UTA finds them more quickly, enabling it to significantly reduce average losses in recent years.

04

4.3 Best practices for fuel card users

For all the efforts of card issuers to protect customers, customers must also protect themselves by ensuring their cards are kept safe and mitigating against misuse.

Here are some best practices for customers to follow:

For drivers:

PIN safety
Card users should memorise their PIN number and never write it down where it could be discovered along with their card. PIN numbers should never be disguised as a date of birth or telephone number on a mobile device, nor should they be divulged to anyone else. In addition, users should shield their PIN when entering it into a payment device.

Card safety
Drivers should never leave their card unattended in the cab of their vehicle or on company premises. Doing so increases the chances of it being copied unknowingly.

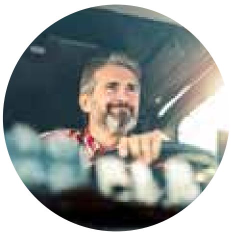
Staying vigilant
Card users should always check the pump for signs of tampering and report anything suspicious. It's safest to use a pump close to a station and in clear view of the cashier and/or CCTV. When paying indoors, card holders should avoid giving their card to the cashier for insertion into a payment device and try to do that themselves. In addition, they should look for suspicious vehicles parked nearby.

For fleet managers:

Card controls
Employers have the capability to set limits on the value spent on their cards and how often they can be used on a daily or monthly basis. Further controls can be set on what products and services can be purchased, and where.

Checking transactions
Employers should check invoices and receipts promptly to ensure that all payments are legitimate. In addition, Kilometres per Litre (KPL) reports for vehicles should be monitored to identify instances of over-consumption.

04

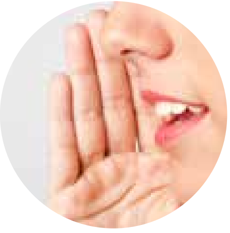


Educating drivers

Employers should educate their drivers about personal accountability; that the misuse of cards is both fraudulent and a criminal offence that could lead to the loss of their job and/ or criminal prosecution. In addition, employers should implement written driver's agreements – documents signed by drivers to show they are aware and have understood the consequences of any misconduct when driving a company vehicle.

Reporting suspicious behaviour or incidents

Employers should file a police report immediately if their drivers are approached by site staff or others to commit fraud or if they have witnessed collusion. In addition, they should report the loss or theft of cards or situations where PIN numbers have been compromised. It's important to report incidents to the police in the country in which the crime was committed as well as in the country of residence. This can expedite cross-border collaboration between forces and potentially lead to a faster, more successful case outcome.



Implementing 'soft' controls

Many companies rely on tip-offs to catch fraudsters. Approximately 43% of incidents are detected because of whistleblowers or other tip-offs[6]. Introducing a whistleblowing system can have economic benefits too: employees and other stakeholders represent the first line of defence against costly misconduct. Early detection provides organisations with the opportunity to address concerns at an early stage and prevent financial penalties and reputational damage.

Fraud often involves employees or senior management who are able to override controls through their high level of authority. Prevention requires a workplace environment that promotes ethical behaviour, deters wrongdoing and encourages employees to communicate any known or suspected wrongdoing to an appropriate person. Would-be fraudsters may not be able to perpetrate certain fraud schemes if employees decline to aid and abet them in committing a crime. Although 'soft' controls to promote appropriate workplace behaviour are more difficult to implement and evaluate than traditional 'hard' controls, they are the best defence against fraud involving senior management.

[6] Source: KPMG

05

How to report card fraud

Answers to frequently asked questions

In case of a suspected or confirmed fraud, please consider the following:

Who should I call in the event of an incident?

Please contact UTA immediately if a transaction via UTA card seems suspicious to you, or if you did not execute the transaction. You can block your card by calling 00 800 88 22 62 26 or via the UTA Service Center. Then file a report with the local police.

Why should I file a report with the police?

Fraud and card misuse for unauthorised transactions are criminal offences. Bear in mind that you may not be the only victim and that the perpetrator may be linked to other serious crimes. To prosecute these scammers, you must report any case of fraud or abuse to the police. The police have far greater powers to investigate and secure evidence than you as an individual.

When should I file a report?

You should contact the police immediately after fraud is discovered as the crime may still be ongoing. Evidence that might be useful to the police, such as video recordings, is usually only kept for a limited period. The retention period may vary depending on the legal requirements of the country in which the crime was committed.

Where should I report the incident?

If you operate internationally, you should consider reporting the incident to the police in the country where the incident occurred and in your home country. That's because in the event of cross-border fraud, the police may need to cooperate for investigations and prosecutions.

What information should I disclose?

Every investigation is different, but employers should be ready to provide information requested by the police, such as:

- Company details, including address and VAT number
- A description of the incident, including the card number/BIN, location, date and time, theft amount
- Details of where the card and PIN are usually kept
- Whether you still have the card
- Whether the card was blocked and if so, when
- Where your drivers were just before the incident – for example: refuelling, parking or taking a break
- Any other relevant piece of information

06 Conclusion

Awareness, vigilance, monitoring, the right technologies, and a rapid response to incidents: All are key factors in minimising fuel card fraud risks.

Fuel card fraud is on the rise and causes significant financial loss to companies every year.

Maintaining up-to-date knowledge about the latest fraud tactics and regional threats, being rigorous in checking transactions and settlements, and ensuring drivers are trained and vigilant can go a long way to safeguarding fleets against fraudsters.

In addition, implementing the right technical tools and security measures can lead to earlier detection of fraud and a faster, more effective response.

Ultimately, the best protection against fuel card fraud rests on ongoing, effective collaboration between fleet operators and fuel card providers.

At UTA, the security and protection of customers comes first. The company will continue to invest and innovate in the pursuit of containing all forms of fraud and minimising risks to customers.

Learn more

For further information about fuel and toll card fraud, or to learn more about UTA policies, security best practices or technology solutions, please contact:

Steffen Glaab

Head of Fraud & Prevention Management

steffen.glaab@uta.com

About UTA

UNION TANK Eckstein GmbH & Co. KG (UTA) is a leading provider of fuel and service cards in Europe. Commercial customers can use the UTA card system to refuel – independent of brand and without cash – at more than 68,000 acceptance points in 40 European countries. The UTA card can also be used for toll invoicing, repair work, and breakdown and towing services. Furthermore, VAT and fuel tax refunds can be claimed through a UTA service provider partner.

UTA was voted „Best fuel card service provider for SMEs 2021" in a survey conducted by German Wirtschaftswoche magazine and the Cologne-based market research institute ServiceValue. UTA was founded in 1963 by Heinrich Eckstein and is today owned by Edenred SE.

For more information: uta.com

About Edenred

Edenred is a leading digital platform for services and payments and the everyday companion for people at work, connecting over 50 million users and 2 million partner merchants in 46 countries via more than 850,000 corporate clients. Edenred offers specific-purpose payment solutions for food (such as meal benefits), mobility (such as multi-energy, maintenance, toll, parking and commuter solutions), incentives (such as gift cards, employee engagement platforms) and corporate payments (such as virtual cards).

True to the Group's purpose, "Enrich connections. For good." these solutions enhance users' well-being and purchasing power. They improve companies' attractiveness and efficiency and vitalize the employment market and the local economy.

They also foster access to healthier food, more environmentally friendly products and softer mobility.

Edenred's 10,000 employees are committed to making the world of work a connected ecosystem that is safer, more efficient and more responsible every day.

In 2020, thanks to its global technology assets, the Group managed close to €30 billion in business volume, primarily carried out via mobile applications, online platforms and cards.

Edenred is listed on the Euronext Paris stock exchange and included in the following indices: CAC Next 20, CAC Large 60, Euronext 100, FTSE4Good and MSCI Europe.

For more information: edenred.com

UNION TANK Eckstein GmbH & Co. KG
Heinrich-Eckstein-Str. 1 - 63801 Kleinostheim - Germany
T/ +49 6027 509-669 - sales@uta.com - uta.com

We connect,
you win