

# Atenție la capcane

Frauda privind cardurile  
de combustibil și modul în  
care poate fi prevenită



# Cuprins

<b>01</b>	Frauda privind cardurile de combustibil în Europa Informații și strategii pentru a asigura securitatea cardurilor și tranzacțiilor	<b>03</b>
<b>02</b>	Tipologia fraudei privind cardurile de combustibil	<b>05</b>
<b>03</b>	Regionalitatea fraudei privind cardurile Puncte fierbinți și tendințe regionale în Europa	<b>10</b>
<b>04</b>	Strategii pentru prevenirea fraudei privind cardurile de combustibil	<b>11</b>
<b>05</b>	Modul de raportare a fraudei privind cardurile Întrebări și răspunsuri frecvente	<b>18</b>
<b>06</b>	Concluzii și alte informații utile	<b>19</b>

## 01

## Frauda privind cardul de combustibil în Europa

Informații și strategii pentru a asigura securitatea cardurilor și tranzacțiilor

Cardurile de combustibil și dispozitivele de plată contactless pentru taxa de drum, au devenit instrumente operaționale cruciale pentru operatorii de transport rutier comercial din Europa dat fiind numărul de autostrăzi, poduri și tuneluri cu taxă din regiune și faptul că șoferii se bazează pe stațiile de alimentare pentru a-i ajuta să ajungă la destinații din întreaga Europă într-o manieră sigură și eficientă.

Dat fiind confortul pe care îl oferă șoferilor, cardurile de combustibil și dispozitivele de plată contactless a taxei de drum, vizibilitatea și controlul pe care acestea le oferă angajatorilor și tendința globală spre metode de plată fără numerar, nu este de mirare că utilizarea acestora este în creștere. Allied Market Research estimează că valoarea pieței globale a cardurilor de combustibil, înregistrată la 672 miliarde de dolari în 2019, aproape se va dubla la 1,2 trilioane de dolari până în 2027.

Cu toate acestea, dezavantajul popularității acestor carduri este riscul de creștere al fraudelor. Desigur, incidentele de fraudă au crescut semnificativ de-a lungul anilor, deoarece infractorii folosesc tehnici din ce în ce mai sofisticate pentru a infiltra securitatea cardurilor și dispozitivelor de plată.

Problema a devenit acută în perioada pandemiei COVID-19, din cauza volumului mare de tranzacții efectuate online. Cazurile de fraudă au crescut în 2020 comparativ cu 2019, cu o creștere semnificativă a cazurilor frauduloase în segmentul taxelor de drum, tuneluri și poduri.

Dat fiind nivelul de consum și prețul combustibilului, precum și dimensiunea multor flote, combustibilul este unul dintre cele mai mari costuri pe care orice operator de transport trebuie să-l suporte și poate reprezenta până la 30% din costurile de administrare ale flotei. Astfel, orice manipulare, utilizare necorespunzătoare sau furt al cardurilor de combustibil poate avea un impact serios asupra profitabilității și un potențial de pierderi de zeci de mii de euro în doar câteva zile.



## 01

**Exemple de fraudă din anii recente:**

- ▶ În 2015, Poliția Criminalistică a Biroului Federal German a arestat un grup infracțional de falsificatori de carduri de combustibil care, conform raportului, a cauzat daune în valoare de 3,5 milioane de euro în Europa prin sustragerea și falsificarea cardurilor.
- ▶ Într-un caz din 2017, autoritățile austriece, împreună cu poliția din Bavaria și din Italia, au investigat opt suspecți care ar fi furat 288 de carduri pentru plata taxelor de drum și de combustibil din camioanele parcate și au cauzat daune în valoare de 1 milion de euro.
- ▶ În 2020, în Germania, un șofer de camion cu două carduri de combustibil deținute a furat motorină în valoare de aproximativ 100.000 de euro.

Ținând cont de aceste lucruri, nu este de mirare că protecția și securitatea împotriva fraudei este un factor important pentru clienți când vine vorba de alegerea unui furnizor de servicii privind cardurile de combustibil.<sup>1</sup>

Obiectivul acestui document este de a oferi managerilor de flote și șoferilor profesioniști informații despre problema fraudei privind cardul de combustibil, pentru a crește astfel conștientizarea privind riscurile de securitate și măsurile de prevenție. Echipa de fraudă și securitate a cardurilor UTA a identificat metodele de operare și punctele fierbinți regionale din Europa, din punct de vedere al fraudelor, prin intermediul cărora sunt comise diferite tipuri de fraude privind cardurile.

**Incidentele de fraudă  
sunt în creștere.**

---

## 02

## Tipologia fraudei privind cardurile de combustibil

### Frauda prin sustragere și copierea cardurilor

Există multe tipuri de fraudă pe care operatorii din segmentul transportului rutier și operatorii de flote trebuie să le cunoască. De departe cel mai comun tip este sustragerea și frauda prin copierea cardului, care însumează împreună majoritatea fraudelor din ultimii trei ani.<sup>2</sup>

Sustragerea și frauda prin copierea cardurilor este situația în care datele cardului sunt furate la un punct de vânzare de către casier sau prin intermediul cititorului de card. Uneori, aceasta se comite în complicitate cu titularul cardului, în schimbul banilor, adesea în zonele de relaxare pentru șoferi. UTA estimează faptul că titularii de carduri complici sunt plătiți cu aproximativ 1.000 de euro / card.

Datele furate sunt folosite pentru a crea o copie a cardului, adesea realizată pentru a imita cardul de combustibil real (poate expirat) pentru a evita suspiciunea în cazul în care sunt opriți și cercetați de către poliție.

Infractorii folosesc tot mai mult tehnologii, precum Bluetooth și Wi-Fi, pentru a transmite datele cardului din dispozitivele de sustragere care au fost introduse în cititoarele de carduri. În mod alternativ, uneori, infractorii instalează dispozitive de blocare în cititoarele de carduri, care împiedică cardurile de la a fi returnate titularului. Acestea sunt folosite împreună cu o cameră mică pentru a capta codul PIN când acesta este introdus.

Când titularul cardului se întoarce la vehicul, infractorul scoate dispozitivul și cardul. Odată copiate, cardurile sunt de obicei utilizate necorespunzător la stații fără personal sau la terminale de plată din exteriorul stațiilor cu personal într-o locație diferită de cea din care au fost sustrate, iar de cele mai multe ori acțiunea se desfășoară în timpul nopții sau în weekend.

Formele mai tradiționale de fraudă prin copierea cardului includ „privirea peste umăr” – caz în care infractorii privesc peste umărul unui utilizator de card care își introduce codul PIN; sau sparg un vehicul parcat, în general dintr-o zonă de relaxare sau un loc dedicat parcării camioanelor, pentru a copia datele cardului. Infractorii știu că șoferii de camioane lasă adesea note adezive în cabinele lor cu datele cardului și codul PIN. Odată ce localizează și copiază informația, aceștia părăsesc vehiculul fără urme, fără ca șoferii să știe că le-au fost compromise cardurile.

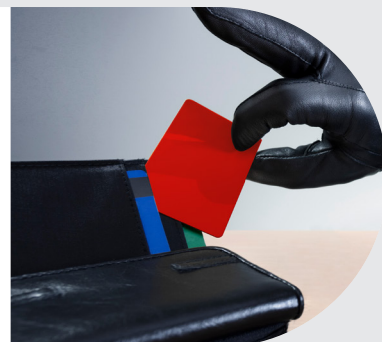
Cardurile cu cip și cod PIN oferă o anumită protecție împotriva sustragerii, însă nu sunt imune din cauza revenirii din prezent la cardurile cu bandă magnetică atunci când cipul este defect sau nu poate fi citit. Infractorii vor defecta cipul zgâriindu-l și punând deasupra lui un sticker fals pentru ca acesta să nu mai poată fi utilizat sau pur și simplu vor zdrobi cipului cardului cu un ciocan.

Sustragerea și copierea cardurilor sunt cele mai comune tipuri de fraudă.

## 02

**Alte tipuri de fraude privind cardurile de combustibil:****Frauda privind cardurile pierdute și furate**

Când infractorii fură carduri și, unde este posibil, coduri PIN. Chiar și fără codul PIN, cardurile furate pot fi folosite în mod fraudulos în rețelele care nu necesită cod PIN, precum achizițiile online. Cele mai multe fraude au legătură cu achizițiile frauduloase cu cardurile anterior descoperirii fraudei sau raportării acestora ca furate, sau achiziții cu cardurile din cauza întârzierii blocării sau restricționării limitelor.

**Complicitatea la locație**

În acest caz, șoferii colaborează cu personalul din locație pentru a tranzacționa combustibil fără a fi efectuată alimentarea sau pentru a solicita mai mult pentru combustibil. Valoarea este adesea schimbată cu numerar sau bunuri, precum țigările. Aceasta este denumită uneori „motorizare”. Cunoștințele despre locurile deschise față de complicitate sunt adesea transmise de la un șofer la altul.

**Abuzul privind utilizarea necorespunzătoare a unui card de către titularul cardului (frauda șoferilor)**

Când un card este folosit pentru alte scopuri decât cele pentru care a fost autorizat. De exemplu, achiziția de combustibil pentru un alt vehicul sau șofer în schimbul banilor; achiziția de combustibil cu un card valid dar decantarea combustibilului din rezervor; folosirea unui „rezervor separat” ascuns în interiorul vehiculului; deteriorarea cipului sau a benzii magnetice pentru a anula controlul de achiziție sau pentru a justifica plata pentru combustibil cu numerar și pentru a ascunde achiziția de bunuri neautorizate; sau șoferi care folosesc datele cardurilor de la alte companii unde au lucrat anterior, etc. Frauda șoferilor este foarte complicat de identificat, deoarece tinde să urmeze comportamentul „uzual” de achiziții al șoferului.

**Fraudă internă**

În acest caz, angajații sau furnizorii acționează singuri sau în complicitate cu părți externe (fie voluntar, fie din cauza constrângerii sau a mitei) pentru a fura date, informații sau materiale de natură sensibilă din punct de vedere comercial sau care ar putea fi folosite pentru a compromite operațiunile sau securitatea companiei.



02

### Frauda privind neprimirea / interceptarea corespondenței

Aceasta implică interceptarea cardurilor și/sau codurilor PIN la adresa clientului, la un hub de sortare a corespondenței sau în cadrul sistemului de distribuție poștală. Cardurile compromise sunt copiate, re-timbrate și livrate clientului. Clienții care sunt supuși celor mai mari riscuri sunt companiile cu căsuțe poștale comune sau cele care își redirectionează corespondența atunci când își schimbă adresa. În mod similar, cardurile și codurile PIN sunt interceptate în hub-urile de sortare a corespondenței din aeroporturi sau din alte părți.



### Frauda privind identitatea și solicitarea

Infractorii uneori își asumă sau preiau identitatea unei companii pentru a deschide un cont folosind documente false sau furate. În cazul în care o solicitare falsă are succes, infractorilor li se emit carduri și acces la alte servicii și li se facturează la termen, oferindu-le astfel suficient timp să comită fraudele. Neplata unei facturi este adesea motivul descoperirii fraudei.



### Frauda privind cardul lipsă

Aceasta implică furtul datelor cardului folosit pentru a face achiziții online, titularul cardului neavând habar de acest lucru până în momentul în care acesta verifică extrasul de cont. Infractorii obțin numerele cardurilor de combustibil folosind programe software speciale care generează numere de card valide, sau prin intermediul sustragerii și încălcării securității datelor și apoi vând cardurile șoferilor, care, la rândul lor, le utilizează în rețelele de taxare. Infractorii (în general foști angajați) vor accesa portalurile online pentru a comanda bilete pentru feribot, eurovinete și taxe de drum folosind datele cardului companiei la care au lucrat anterior pentru vehiculele unei alte companii (în general pentru actualul angajator sau posibil pentru un șofer proprietar cu care colaborează).



### Clonarea vehiculului

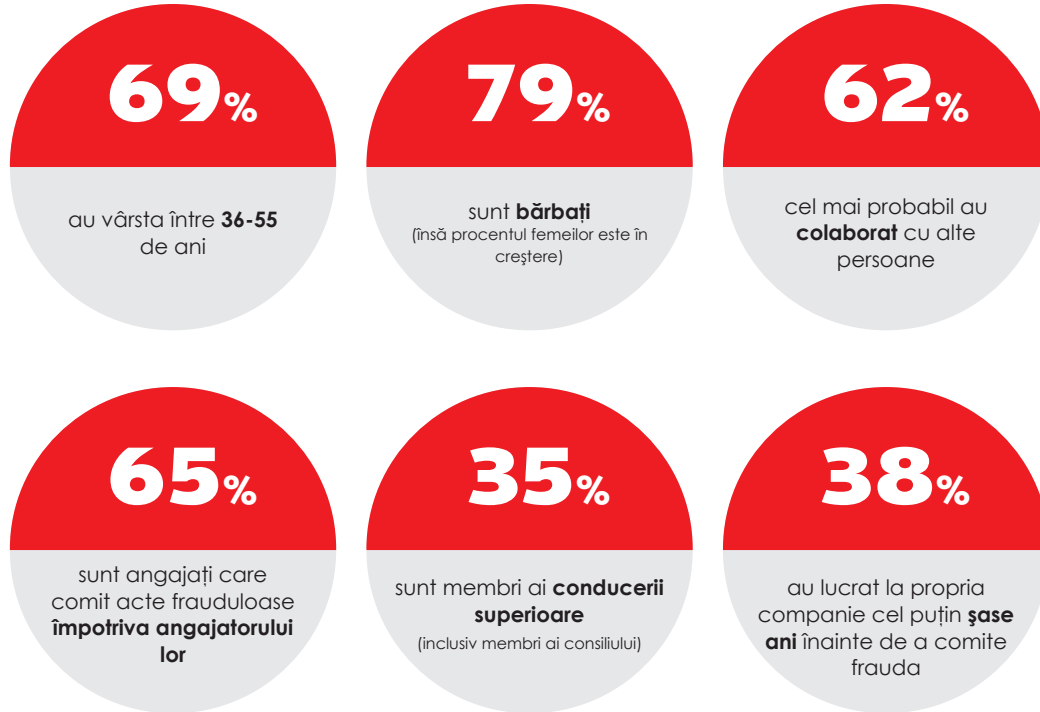
În acest scenariu, numărul de înmatriculare al unui vehicul este copiat și folosit pentru un alt vehicul cu aceeași marcă și model, în scopul evitării plății de combustibil, taxei de drum și de parcare, taxelor de trafic și multe altele.



02

## Profilul infractorului

Următoarele caracteristici sunt comune infractorilor<sup>3</sup>:



Frauda la scară largă implică de obicei membri ai conducerii care anulează auditul procesului prin intermediul gradului înalt de autoritate.

### În plus, în general infractorii:

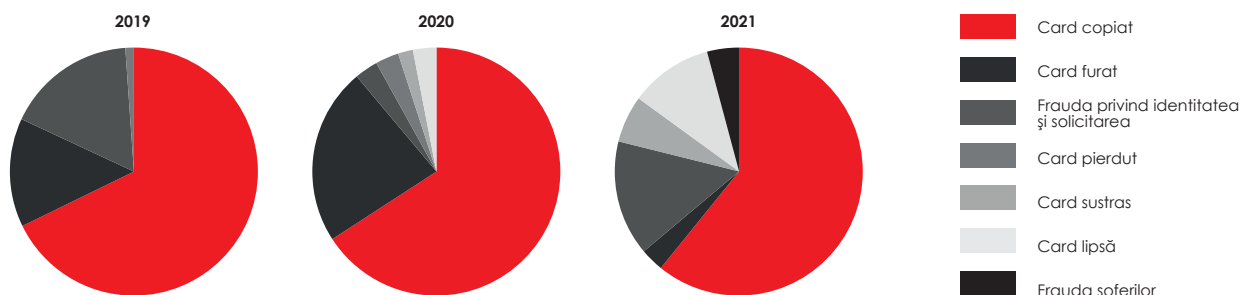
- ▶ Nu își iau vacanțe
- ▶ Sunt secretoși cu privire la procesele comerciale
- ▶ Se opun supravegherii
- ▶ Au aptitudini personale slabe
- ▶ Au abilități tehnice bune
- ▶ Lucrează până târziu
- ▶ Sunt predispuși la abuz de substanțe/alcool
- ▶ Sunt predispuși la certuri și divergențe



02

## Exemple privind evoluția fraudelor în Europa 2019-2021

Contribuția tipului de fraudă la pierderile totale pe ani



Deoarece amenințările de fraudă sunt în continuă schimbare, evaluările periodice privind riscurile și evoluția continuă a metodelor de prevenire și detectare sunt vitale pentru menținerea unor niveluri ridicate de securitate

### Frauda privind cardurile evoluează:

- ▶ De la infractori individuali până la grupuri internaționale de infracționalitate organizată.
- ▶ De la sustragerea unui singur card până la atacuri de încălcare a securității datelor.
- ▶ De la infractori care lucrează pe tot parcursul ciclului de viață al fraudei până la infractori specializați în parte în acel lanț valoric și care vând această valoare la nivelul următor.

### Infractorii devin din ce în ce mai sofisticăți prin intermediul:

- ▶ Dispozitivelor de falsificare
- ▶ Manipulării locației
- ▶ Amenințărilor
- ▶ Asumării unor identități digitale frauduloase
- ▶ Mascarea în clienți
- ▶ Oferirea fraudei ca serviciu (FaaS) adesea prin intermediul dark web-ului – realizată fie prin sindicate globale de criminalitate, fie de infractori individuali



## 03

## Regionalitatea fraudei privind cardurile

## Puncte fierbinți și tendințe regionale în Europa

În epoca digitală actuală, tehnicile de fraudă sunt din ce în ce mai sofisticate pe zi ce trece. În trecut, infractorii de obicei copiau un singur card de combustibil, însă, în prezent, adesea produc mai multe versiuni și le distribuie simultan în diferite țări pentru un câștig financiar maximum. Pentru a reuși o astfel de acțiune, infractorii trebuie să fie organizați. Și bineînțeles, mulți dintre ei fac adesea parte din grupări mai mari implicate în trafic de droguri, trafic de persoane, trafic de arme sau chiar mai rău.

Grupările organizate sunt foarte răspândite în toată Europa<sup>4</sup> și multe dintre ele au adoptat o concentrare geografică în eforturile lor privind fraudă. Analiza indică faptul că o grupare se axează pe stațiile de alimentare de pe autostrăzi la principalele joncțiuni est-vest sau nord-sud din Franța, în timp ce alta se concentrează pe granița de sud a Olandei, la granița cu Belgia și Germania. Cele mai recente constatări indică activități infracționale crescute semnificativ pe ruta din Bordeaux către Irun, în Spania, pe coasta de est din Italia și pe rutele care duc din Italia către Slovenia. De asemenea, granița Franței cu Germania și Elveția a avut o creștere a incidentelor de fraudă privind cardurile în ultimele luni.

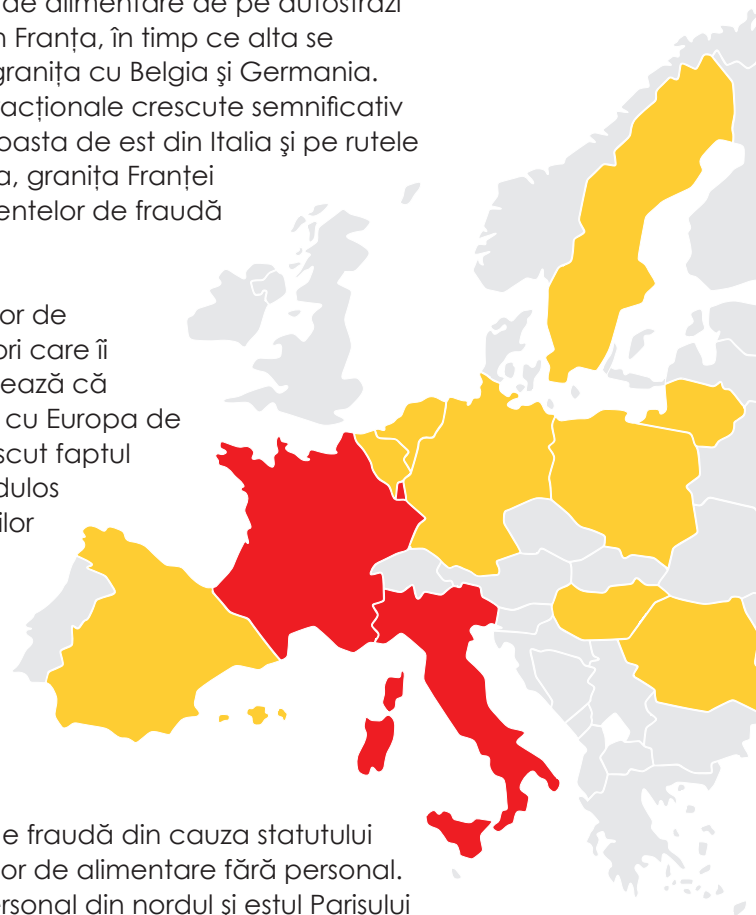
Totuși, alte grupări se axează pe șoferii din țara lor de origine, țări în care aceștia pot avea colaboratori care îi ajută să comită fraude. De exemplu, se suspectează că grupările din Franța și Olanda pot avea legături cu Europa de Est și pot viza șoferi din acea regiune. Este cunoscut faptul că majoritatea eurovinetelor achiziționate fraudulos online sunt pentru vehicule ce aparțin companiilor cu sedii în Europa de Est.

În general, fraudă reflectă succesul companiilor de transport din Europa de Est, care transportă mărfuri spre vest și sud prin Italia și Franța, spre Spania și spre nord, în Scandinaviei și retur.

Franța, în special, a devenit un punct fierbinte de fraudă din cauza statutului său de centru de transport și a prevalenței stațiilor de alimentare fără personal. Majoritatea sustragerilor au loc în stațiile fără personal din nordul și estul Parisului și în principalele noduri de transport din jurul orașelor Lyon și Grenoble. Mai în sud, Perpignan a observat o creștere a infracțiunilor în primul trimestru al anului 2021.

Stațiile de alimentare și zonele de relaxare de-a lungul graniței dintre Franța și Spania și în zona de graniță Venlo din Olanda sunt principalele locații pentru spargerile de vehicule și utilizarea necorespunzătoare a cardurilor copiate.

Monitorizarea evenimentelor de fraudă și a distribuției geografice sunt utile în prevenirea fraudei și în capacitatea de a reacționa rapid dacă acestea au loc.



**Puncte fierbinți  
de fraudă  
2019 - 2021**

<sup>4</sup> Sursa Europol: Un singur atac de copiere în masă din Olanda ce exploatează lacunele privind viteza a furat 800.000\$ în câteva săptămâni. În Italia, un atac în cadrul limitelor privind viteza la locație a furat 3,2 milioane de dolari în mai puțin de două luni. În 2018, Europol a prins un grup criminal spaniol ce folosea carduri de combustibil contrafăcute în rețelele de taxare spaniole și franceze: Au fost efectuate 24 de arestări, au fost compromise 600 de înregistrări de vehicule, au fost dezasamblate 11 fabrici de carduri, au fost sechestrate 15.000 de carduri contrafăcute și a fost identificată o pierdere de 500.000€.

## 04

## Strategii pentru prevenirea fraudei privind cardurile de combustibil

Ce se poate face pentru a reduce riscul fraudei privind cardurile și pentru a împiedica eforturile în continuă evoluție ale infractorilor? În primul rând, emitenții de carduri, managerii flotelor, partenerii și utilizatorii cardurilor trebuie să lucreze împreună pentru a obține cele mai înalte nivele de securitate.

### 4.1 Măsurile pentru furnizorii de carduri de combustibil

Deoarece frauda privind cardurile de combustibil a devenit o amenințare în toată Europa condusă de grupările internaționale, detectarea și acționarea în justiție necesită colaborarea instituțiilor și a autorităților internaționale. Două autorități majore din acest domeniu sunt Biroul de investigare a fraudei privind cardurile de combustibil din industrie (FICFIB), un grup de emitenți de carduri, retailerii de combustibil și operatori de stații de servicii independente care distribuie informații privind tendințele, vulnerabilitățile și amenințările în curs de dezvoltare; și Europol, care distribuie informații privind incidentele transfrontaliere către forțele de poliție locale pentru a asista la incidentele și la investigațiile privind clienții. Colaborarea strânsă cu instituțiile oferă furnizorilor de carduri influența internațională de care au nevoie pentru acțiuni de succes în cazul unui incident.

În plus, față de colaborarea cu autoritățile și instituțiile, este crucial pentru furnizorii de carduri să stabilească, să monitorizeze constant și, dacă este necesar, să-și optimizeze produsele, serviciile și procesele. Aceasta începe cu proiectarea de produse și servicii, precum notificările privind tranzacțiile, și include calificarea regulată a serviciului pentru clienți și a proceselor IT, pentru a se asigura că activitatea infracțională în timp real poate fi contracarată cât mai repede posibil.

În final, comunicarea este o componentă crucială a securității cardurilor. Procesele de comunicare cu autoritățile, partenerii și clienții trebuie să fie rapide și concentrate.

În cazul unei fraude, comunicarea rapidă cu orice persoană afectată este crucială. Mai mult, este important să creștem conștientizarea printre clienți și parteneri despre pericolele fraudei privind cardurile de combustibil și să le oferim asistență în prevenirea acesteia.

## 04

## 4.2 Abordarea UTA cu privire la prevenirea fraudei privind cardurile de combustibil

În calitate de furnizor de servicii de mobilitate, cardurile de combustibil și servicii reprezintă piatra de temelie a portofoliului de produse și servicii UTA. În consecință, securitatea cardurilor și a tranzacțiilor este o prioritate.

În centrul eforturilor anti-fraudă ale UTA se află echipa sa dedicată fraudei și securității cardurilor care acoperă responsabilități precum:

- ▶ Notificările tranzacțiilor în timp real ce permit clienților să intervină imediat
- ▶ Alertarea clienților prin telefon în cazul detectării de evenimente suspecte
- ▶ Dezvoltarea și implementarea de strategii și procese pentru detectarea, prevenirea și atenuarea eficientă a fraudei
- ▶ Recomandarea tehnicilor pentru limitarea riscului de fraudă
- ▶ Colaborarea cu avocați, agenți de poliție, FICFIB și alții pentru a dezvolta și executa planuri pentru soluționarea cazurilor de fraudă
- ▶ Dezvoltarea și monitorizarea rapoartelor și informațiilor utile în prinderea infractorilor
- ▶ Realizarea de interviuri cu victimele și suspecții pentru a obține informații cu privire la tipul de atac și pentru a determina implicarea lor potențială



“

*Prin intermediul produselor, serviciilor și proceselor noastre ne angajăm să ne protejăm clienții împotriva formelor actuale și emergente de fraudă.”*

Carsten Bettermann, Director Executiv al UTA



Securitatea cardurilor și tranzacțiilor reprezintă factorii cheie de succes din sectorul serviciilor de mobilitate.

## 04

## Valorificarea informațiilor din industrie

Un motiv pentru rata mare de detectare a fraudei de către UTA este experiența acumulată prin ani de colaborare cu organizații de securitate de top, organisme din industrie și experți terți.

În cazul în care UTA nu are expertiză internă, aceasta colaborează cu specialiști, de exemplu, în domenii precum criminalistica cibernetică, amenințări emergente privind cardurile de plată și produsele bancare, web trawling sau investigații criminalistice profunde. De exemplu, pentru detectarea automată și optimizată bazată pe algoritmi, UTA colaborează cu The ai Corporation Ltd, o companie specializată în sisteme bazate pe inteligență artificială pentru securitatea plăților și monitorizarea tranzacțiilor. De asemenea, UTA este membru al FICFIB, colaborează cu Europol și este membru activ al organismelor din industrie care stabilesc standardele comune pentru schimbul de date sigur dintre rețelele de acceptanță și emitenții de carduri.

Mai mult, UTA lucrează cu operatorii din stațiile de alimentare și servicii din 40 de țări europene pentru a se asigura că aceștia respectă regulile de securitatea în propriile locații, precum camere CCTV sau prin IP, protecții împotriva instalării de dispozitive de sustragere și capacități de autorizare a tranzacțiilor online.

Ca parte din grupul Edenred, UTA beneficiază de expertiză în domenii precum conformitate, confidențialitatea datelor și securitate IT. Forumul privind fraudă de lungă durată al Edenred se întinde pe toate liniile sale de activitate în peste 50 de țări, împărtășind informații și cele mai bune practici pe subiecte de la tipuri de fraudă până la litigii.



“

*Inteligența artificială și învățarea automatizată sunt instrumente indispensabile din prezent pentru a preveni în mod eficient fraudă privind cardurile de combustibil și pentru a detecta rapid cazurile de fraudă. În cadrul colaborării noastre cu UTA, combinăm sistemele tehnice de ultimă generație (aiAutoPilotML) și cunoștințele experților noștri în carduri de combustibil, cu experiența cuprinzătoare pe care UTA o aduce în domeniul prevenirii și detectării fraudei privind cardurile de combustibil. Prin intermediul acestei combinații de tehnologie, expertiză și cunoștințe ale experților, obținem un impact și o rată de succes foarte mare în legătură cu prevenirea și combaterea fraudei privind cardurile de combustibil.”*

Dr. Mark Goldspink,  
Director Executiv al The ai  
Corporation Ltd

Combinarea expertizei interne cu colaborări cu partenerii specializați pentru a obține rezultate.

## 04

**Asumarea unei atitudini proactive, de prevenție**

Pe lângă experiența sa în acest subiect, UTA are o abordare de prevenție, de tipul „securitate personalizată”, pentru a se asigura că platformele și produsele sunt construite de la bază pentru o securitate maximă. În plus, compania investește semnificativ în cercetare și dezvoltare în domenii precum analiza datelor, inteligența artificială și învățare automatizată pentru a-și ajuta Echipa de fraudă și securitatea cardurilor să detecteze o gamă mereu extinsă de tipuri de fraudă cât mai repede posibil.

De exemplu, pentru a combate falsificarea în masă a cardurilor de combustibil și de plată a taxelor, UTA a implementat verificări de plauzibilitate geografică ce monitorizează timpul și distanța dintre locații pentru a vedea dacă este fizic posibil pentru ca o tranzacție să fie legitimă sau nu. Când sunt identificate probleme, cardurile sunt blocate imediat, iar clienții sunt informați.

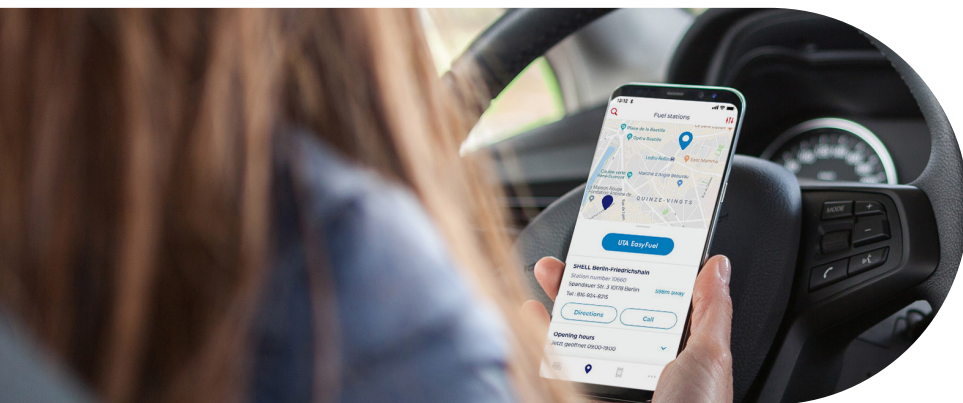
O asemenea vizibilitate granulară a peisajului de fraudă din Europa permite Echipei de fraudă și securitatea cardurilor să acționeze pentru a minimiza riscul clienților, pentru a solicita asistența Europol și a altor autorități competente, dacă este necesar, și pentru a împărtăși informații în cadrul FICFIB.



“

*Actualmente dezvoltăm noul nostru card de combustibil digital. Această soluție avansată combină experiența UTA în securitatea tranzacțiilor și prevenirea fraudei cu cunoștințele aprofundate ale companiei noastre mamă Edenred cu privire la serviciile de plată.”*

Carsten Bettermann,  
Director Executiv al UTA



### Cardurile de combustibil digitale - mai rapide, mai comode și mai sigure

Procedurile de plată digitală contactless sunt în creștere - o tendință accelerată de pandemia COVID-19. Aplicațiile privind cardurile de combustibil digitale pe un smartphone nu permit doar achiziții mai ușoare la pompă ci asigură și procese mai rapide și mai eficiente, de la autentificarea și înregistrarea în sistem până la gestionarea datelor și rezervărilor proprii.

Un alt avantaj este reprezentat de nivelul adițional de securitate a tranzacțiilor pe care aceste carduri digitale îl oferă în comparație cu cardurile de combustibil fizice.

## 04

**Reducerea riscurilor clienților**

Pentru a reduce riscurile de fraudă privind cardurile clienților, UTA a implementat o serie de funcții și servicii de securitate. Acestea includ blocarea cardului 24/7 prin intermediul portalului online UTA, coduri PIN pentru toate cardurile, permiterea clienților să-și seteze propriile limite de cheltuieli, control privind locul și ora la care pot fi achiziționate produsele și facturare și raportare transparentă. Clienții pot limita suma de pe card pe care o pot folosi pentru achiziții și pot limita zilele săptămânii și orele în care acesta poate fi folosit.

Serviciul de notificare a tranzacției UTA alertează clienții în timp real atunci când se fac tranzacții cu cardurile de combustibil UTA, permițându-le să intervină în cazul în care constată ceva suspect. Serviciul poate fi personalizat pe cerințele clientului, de exemplu, pot fi setate filtre pentru a trimite notificări prin mesaj sau email, se poate seta o valoare minimă per tranzacție pentru orice alertă, sau se poate seta o dată specifică țării sau restricții de timp.

În cele din urmă, UTA sprijină clienții care sunt victime ale fraudei contactând furnizorul, de exemplu, operatorul stației de combustibil, pentru a solicita ca acesta să salveze orice filmare sau video CCTV pentru investigațiile poliției. Unde este cazul, Echipa de fraudă și securitatea cardurilor a UTA va colabora cu poliția pentru a furniza informații ce pot fi folosite ca dovezi sau pentru a identifica alte victime potențiale.

**O istorie de succes**

Pe scurt, UTA depune tot efortul necesar să anticipeze, să identifice și să neutralizeze activitatea infracțională înainte ca aceasta să afecteze clienții, o atitudine în urma căreia compania se bucură de o rată mare de succes. Compania identifică aproximativ 90% din incidente înainte ca acestea să fie observate de clienți. Acum doi ani, această cifră era de 63%, evidențiind eficacitatea eforturilor companiei. Pe lângă identificarea multor incidente de fraudă, UTA le găsește mai rapid, fiind capabilă să reducă semnificativ pierderile medii din ultimii ani.

## 04

### 4.3 Cele mai bune practici pentru utilizatorii cardurilor de combustibil

Pe lângă toate eforturile emițătorilor de carduri de a-și proteja clienții, aceștia trebuie, de asemenea, să se protejeze, asigurându-se că păstrează cardurile în siguranță și diminuează utilizarea necorespunzătoare.

**Iată câteva dintre cele mai bune practici pe care clienții ar trebui să le respecte:**

#### Pentru șoferi:



##### Siguranța codului PIN

Utilizatorii de carduri ar trebui să memoreze codul PIN și niciodată să nu-l scrie undeva unde ar putea fi descoperit împreună cu cardul lor. Codurile PIN nu ar trebuie să fie niciodată camuflate ca data nașterii sau numărul de telefon de pe un dispozitiv mobil și nici nu ar trebuie să fie divulgate altor persoane. În plus, utilizatorii trebuie să-și acopere codul PIN atunci când îl introduc într-un dispozitiv de plată.



##### Siguranța cardului

Șoferii nu trebuie să își lase cardul niciodată nesupravegheat în cabina vehiculului lor sau la sediul companiei. Acest lucru crește șansele ca acesta să fie copiat fără ca aceștia să știe.



##### Rămâneți vigilenți

Utilizatorii de carduri trebuie să verifice întotdeauna pompa pentru semne de interferențe și să raporteze orice lucru suspect. Este mai sigur să folosiți o pompă aproape și la vedere pentru casier și/sau camera de luat vederi. Când plătesc în interior, titularii cardurilor trebuie să evite să dea cardul casierului pentru a-l introduce în dispozitivul de plată și să încerce să facă acest lucru ei înșiși. În plus, aceștia trebuie să se uite după vehicule suspecte parcate în apropiere.

#### Pentru managerii de flote:



##### Limitarea cardurilor

Angajatorii au posibilitatea de a seta limite pe valoarea cheltuită cu cardurile lor și frecvența utilizării zilnice sau lunare. Pot fi setate și alte tipuri de limitări în funcție de tipul produselor și serviciilor ce pot fi achiziționate și locațiile aferente.



##### Verificarea tranzacțiilor

Angajatorii trebuie să verifice facturile și chitanțele cu promptitudine pentru a se asigura că toate plățile sunt legitime. În plus, rapoartele Kilometri per litru (KPL) trebuie monitorizate pentru a identifica situațiile de consum în exces.



04



### Educarea șoferilor

Angajatorii trebuie să-și educe șoferii cu privire la răspunderea personală; privind faptul că utilizarea necorespunzătoare este frauduloasă și reprezintă o infracțiune penală ce poate duce la pierderea locului de muncă și /sau la urmărire penală. În plus, angajatorii trebuie să implementeze acordurile scrise ale șoferilor - documentele semnate de către șoferi care demonstrează că aceștia cunosc și au înțeles consecințele oricărui comportament necorespunzător la conducerea unui vehicul al companiei.



### Raportarea comportamentelor sau incidentelor suspecte

Angajatorii trebuie să depună imediat plângere la poliție dacă șoferii lor sunt abordați de personalul locației sau de alte persoane pentru a comite o fraudă sau dacă au fost martori la complicitate. În plus, aceștia trebuie să raporteze pierderea sau furtul cardurilor sau a situațiilor în care codurile PIN au fost compromise. Este important să raporteze incidentele poliției din țara în care a fost comisă infracțiunea, precum și poliției din țara de reședință. Acest aspect poate grăbi colaborarea transfrontalieră și poate duce la un rezultat mai rapid și de succes al cazului.



### Implementarea controalelor „lejere“

Multe companii se bazează pe ponturi pentru a prinde infractorii. Aproximativ 43% dintre incidente sunt detectate datorită informatorilor sau a altor tipuri de informații<sup>5</sup>. Introducerea unui sistem de avertizare poate avea și avantaje economice: angajații și alte părți interesate reprezintă prima linie de apărare împotriva unei conduite necorespunzătoare costisitoare. Detectarea timpurie oferă organizațiilor oportunitatea de a adresa îngrijorările într-o etapă inițială și previne penalizările financiare și daunele reputaționale.

Frauda implică adesea angajații sau conducerea superioară care poate anula controalele prin nivelul ridicat de autoritate. Prevenția necesită un mediu de lucru care promovează comportamentul etic, descurajează acțiunile greșite și încurajează angajații să comunice orice acțiune greșită cunoscută sau suspectă către persoana potrivită. Infractorii ar putea să nu comită anumite scheme de fraudă dacă angajații refuză să îi ajute la comiterea unei infracțiuni. Deși controalele „lejere” pentru promovarea unui comportament adecvat la locul de muncă sunt mai dificil de implementat și de evaluat decât controalele „serioase” tradiționale, acestea sunt cea mai bună apărare împotriva fraudei ce implică conducerea superioară.

## 05

## Modul de raportare a fraudei privind cardurile

Întrebări și răspunsuri frecvente

**În cazul unei fraude suspecte sau confirmate, vă rugăm să aveți în vedere următoarele:**

### **Pe cine trebuie să sun în cazul unui incident?**

Vă rugăm să contactați UTA imediat dacă o tranzacție prin cardul UTA vi se pare suspectă sau dacă nu ați realizat dvs. tranzacția. Puteți bloca cardul sunând la 00 800 88 22 62 26 sau prin Contul de Client UTA. Apoi depuneți o plângere la poliția locală.

### **De ce trebuie să depun o plângere la poliție?**

Frauda și utilizarea necorespunzătoare a cardului pentru tranzacții neautorizate reprezintă infracțiuni penale. Rețineți că este posibil ca dvs. să nu fiți singura victimă și că infractorul poate fi legat de alte infracțiuni majore. Pentru a urmări acești falsificatori, este nevoie să raportați orice caz de fraudă sau abuz poliției. Poliția are putere mult mai mare de investigare și de asigurare a dovezilor decât dvs. ca individ.

### **Când trebuie să depun plângerea?**

Trebuie să contactați poliția imediat după ce a fost descoperită frauda, deoarece infracțiunea poate fi încă în curs. Dovezile ce pot fi utile poliției, precum înregistrările video, sunt păstrate de obicei doar pentru o perioadă limitată. Perioada poate varia în funcție de cerințele legale din țara în care a fost comisă infracțiunea.

### **Unde trebuie să raportați incidentul?**

Dacă aveți activitate internațională, trebuie să aveți în vedere raportarea incidentului poliției din țara în care a avut loc incidentul și poliției din țara de reședință. Deoarece, în cazul unei fraude transfrontaliere, poliția poate avea nevoie să colaboreze pentru investigații și urmări.

### **Ce informații trebuie să divulgați?**

Fiecare investigație este diferită, însă angajatorii trebuie să fie pregătiți să furnizeze informațiile solicitate de către poliție, precum:

- ▶ Datele companiei, inclusiv adresa și codul fiscal
- ▶ O descriere a incidentului, inclusiv numărul de card/BIN, locația, data și ora, suma furată
- ▶ Detaliile cu privire la locurile în care este păstrat de obicei cardul și codul PIN.
- ▶ Dacă încă mai aveți cardul
- ▶ Dacă cardul a fost blocat și dacă răspunsul este afirmativ, când?
- ▶ Unde se aflau șoferii dvs. înainte de incident, de exemplu: realimentau, parcau sau luau o pauză
- ▶ Orice alte informații relevante

## 06

## Concluzie

Conștientizarea, vigilența, monitorizarea, tehnologiile potrivite și un răspuns rapid la incidente: toți sunt factori cheie în minimizarea riscurilor de fraudă cu cardurile de combustibil.

Frauda cu cardurile de combustibil este în creștere și cauzează pierderi financiare semnificative în fiecare an.

Menținerea cunoștințelor actualizate despre cele mai recente tactici de fraudă și amenințări regionale, verificarea riguroasă a tranzacțiilor și deconturilor, asigurarea că șoferii sunt instruiți și vigilenți pot fi instrumente utile pentru protejarea flotelor împotriva infractorilor.

În plus, implementarea instrumentelor tehnice și a măsurilor de securitate potrivite poate duce la detectarea timpurie a fraudei și la un răspuns mai rapid și mai eficient.

În cele din urmă, cea mai bună protecție împotriva fraudei privind cardurile de combustibil este colaborarea continuă și eficientă dintre operatorii de flote și furnizorii de carduri de combustibil.

În cadrul UTA, securitatea și protecția clienților este pe primul loc. Compania va continua să investească și să inoveze în demersul de a stopa orice formă de fraudă și de a minimiza riscurile pentru clienți.

### Aflați mai multe

Pentru informații suplimentare despre fraudele cu cardurile de combustibil sau pentru a afla mai multe despre politicile UTA, despre cele mai bune practici de securitate sau soluții tehnologice, vă rugăm să-l contactați pe:

**David Jones**

Director Securitate Plăți și  
Dezvoltare Corporativă UTA,  
Soluții pentru Flote și Mobilitate,  
Edenred

david.jones@edenred.com

## Despre UTA

**UNION TANK Eckstein GmbH & Co. KG (UTA)** este unul dintre liderii pe piața cardurilor de combustibil și serviciilor din Europa. Companiile client pot folosi sistemul de carduri UTA pentru a alimenta cu combustibil, fără numerar, în peste 68.000 de stații de alimentare din diverse rețele, în 40 de țări europene și pot beneficia de alte servicii precum decontarea taxelor de drum, servicii de reparații, servicii de intervenție în caz de pană și tractare. În plus, rambursările de TVA și accizele pe combustibil pot fi solicitate prin intermediul unui partener UTA, furnizor de servicii specializate.

UTA a fost votat „Cel mai bun furnizor de carduri de combustibil pentru IMM-uri 2021” într-un sondaj realizat de revista germană *Wirtschaftswoche* și de institutul de cercetare a pieței ServiceValue. Compania, care a fost înființată în 1963 de Heinrich Eckstein, este deținută astăzi de Edenred SE.

**Pentru mai multe informații: [uta.com](http://uta.com)**

## Despre Edenred

**Edenred** este lider de piață ca platformă de servicii și plăți și este partenerul de zi cu zi al întregului ecosistem al pieței muncii, conectând peste 50 de milioane de angajați și 2 milioane de comercianți parteneri prin intermediul a peste 850.000 de clienți corporativi în 46 de țări.

Edenred oferă soluții de plată cu destinații specifice pentru alimentație (tichete de masă), flote auto și mobilitate (carduri de combustibil, soluții multi-energy, mentenanță, taxe de drum, parcări și vouchere de transport), stimulente (vouchere și carduri cadou, platforme dedicate angajaților) și plăți corporative (carduri de plată virtuale).

În concordanță cu misiunea grupului, "Enrich connections. For good.", aceste soluții sporesc bunăstarea și puterea de cumpărare a utilizatorilor. Îmbunătățesc atractivitatea și eficiența companiilor și animă piața muncii și economia locală.

De asemenea, favorizează accesul la o alimentație mai sănătoasă, produse mai sustenabile și soluții de soft mobility.

Cei 10.000 de angajați Edenred sunt conduși de misiunea comună de a transforma piața muncii într-un ecosistem interconectat, mai sigur, mai eficient și mai prietenos zi de zi.

În 2020, datorită activelor sale tehnologice globale, Grupul a gestionat un volum de afaceri de 30 miliarde de euro, efectuat în principal prin aplicații mobile, platforme online și carduri.

Edenred este cotată la bursa de valori Euronext Paris și este inclusă în următorii indicatori: CAC Next 20, CAC Large 60, Euronext 100, FTSE4Good și MSCI Europe.

**Pentru mai multe informații: [edenred.com](http://edenred.com)**