Vorsicht Falle:

Tankkartenbetrug und wie Sie sich davor schützen

Tankkarte? Aber sicher!
Betrug erkennen und vermeiden

INHALTE

01

Tankkartenbetrug in Europa

Infos und Strategien für mehr Sicherheit bei Karten und Transaktionen

Tankkarten und On-Board Units zur kontaktlosen Mautabwicklung sind unverzichtbare Hilfsmittel für international operierende Transportunternehmen. Mit ihrer Hilfe tanken Fahrer bargeldlos und komfortabel und wickeln bequem die Maut für die zahlreichen kostenpflichtigen Autobahnen, Brücken und Tunnel in ganz Europa ab.

Neben den praktischen Vorteilen, die Tankkarten und Mautboxen den Fahrern bieten, profitieren auch die Fuhrunternehmen und deren Buchhaltung von der Transparenz und den Kontrollmöglichkeiten, die diese Hilfsmittel mit sich bringen. Verbunden mit dem generellen weltweiten Trend hin zu bargeldlosen Zahlungs- und Abwicklungsverfahren überrascht es nicht, dass die Nutzung von Tankkarten und Mautboxen konstant zunimmt. Schätzungen von Allied Market Research zufolge wird sich das Volumen des globalen Tankkartenmarkts, das 2019 bei 672 Milliarden US-Dollar lag, bis zum Jahr 2027 auf 1,2 Billionen US-Dollar nahezu verdoppeln.

Die Kehrseite der weiten Verbreitung von Tank- und Servicekarten ist jedoch das steigende Betrugsrisiko. Betrugsdelikte im Zusammenhang mit Tankkarten haben in den letzten Jahren signifikant zugenommen, da Kriminelle immer versiertere Strategien anwenden, um die Sicherheit von Tankkarten zu unterwandern.

Dieses Problem hat sich während der COVID-19-Pandemie noch verschärft, da im allgemeinen Bestreben nach Kontaktvermeidung der Trend zu Online-Transaktionen stark zugenommen hat. So ist die Zahl der Betrugsfälle im Jahr 2020 im Vergleich zum Jahr 2019 merklich gestiegen. Ein Großteil dieses Anstiegs wurde bei Betrugsfällen in Verbindung mit Mautgebühren sowie den Nutzungskosten für Tunnel und Brücken verzeichnet.

Angesichts des Verbrauchs moderner Lkw, der Treibstoffpreise sowie der Größe vieler Fuhrparks ist Kraftstoff einer der größten Kostenfaktoren von Transportunternehmen. Treibstoff kann bis zu 30 % der laufenden Kosten eines Fuhrparks ausmachen. Daher kann jede Manipulation, jeder Missbrauch und jeder Diebstahl von Tankkarten hohe wirtschaftliche Schäden verursachen. Verluste in Höhe von Zehntausenden von Euros innerhalb weniger Tage sind möglich.

01

Hier einige Beispiele aus den letzten Jahren:

- 2015 verhafteten Ermittlungsbeamte des BKA eine Bande von Tankkartenfälschern, die Berichten zufolge Schäden in Höhe von 3,5 Mio. Euro in ganz Europa durch Karten-Skimming verursacht hatten.
- In einem Fall aus dem Jahr 2017 ermittelten die österreichischen Behörden in Kooperation mit der bayerischen und italienischen Polizei gegen acht Verdächtige, denen vorgeworfen wurde, 288 Maut- und Tankkarten aus geparkten LKW gestohlen und Schäden in Höhe von 1 Mio. Euro verursacht zu haben.
- 2020 stahl in Deutschland ein LKW-Fahrer mit zwei manipulierten Tankkarten Diesel im Wert von ca. 100.000 Euro.

Vor diesem Hintergrund ist es kein Wunder, dass für Kunden von Mobilitätsdienstleistern Sicherheit und Betrugsprävention entscheidende Faktoren für die Auswahl eines Tankkartenanbieters sind.[1]

Das Ziel dieses Whitepapers ist es, Fuhrparkmanagern und Berufskraftfahrern Einblicke in das Thema Tankkartenbetrug zu bieten, um ihr Bewusstsein für Sicherheitsrisiken und Schutzmaßnahmen zu wecken. UTAs Betrugs- und Kartensicherheitsteam hat die verschiedenen Methoden des Tankkartenbetrugs aufgeschlüsselt und regionale Hotspots für Tankkartenbetrug in Europa identifiziert.

Die Fallzahlen von Tankkartenbetrug nehmen zu.

1 Quelle: Datamonitor

02 Formen des Tankkartenbetrugs

Skimming und Betrug mit kopierten Karten

Es gibt zahlreiche Typen des Tankkartenbetrugs, die Transport- und Fuhrparkunternehmer kennen sollten. Die bei weitem häufigste Betrugsart ist das Skimming und Kopieren von Karten. Die Mehrzahl aller Betrugsfälle in den letzten drei Jahren entfällt auf diesen Typ.[2]

Beim Skimming und Kopieren von Karten werden Kartendaten während einer POS-Transaktion vom Kassenpersonal oder über das Kartenlesegerät gestohlen. Manchmal wird dieser Betrug zusammen mit dem Karteninhaber im Tausch gegen Geld begangen, häufig auf Rastplätzen für Kraftfahrer. Rund 1.000 Euro pro Karte werden dabei nach Schätzungen von UTA von Kriminellen an kooperierende Kartenhalter gezahlt.

Die gestohlenen Daten werden zur Herstellung einer kopierten Karte verwendet, die häufig einer echten oder abgelaufenen Tankkarte nachempfunden ist, um zum Beispiel bei einer Polizeikontrolle keinen Verdacht zu erregen.

Zunehmend finden Techniken wie Bluetooth oder WiFi Verwendung, um Kartendaten von Skimming-Vorrichtungen zu übertragen, die in Kartenleser eingesetzt wurden. Teils bauen Kriminelle auch Vorrichtungen in die Kartenlesegeräte ein, die verhindern, dass die Karte nach Abschluss des Vorgangs wieder ausgegeben wird. Solche Vorrichtungen werden in Verbindung mit einer kleinen Kamera verwendet, um die PIN-Nummer während der Eingabe zu erfassen. Wenn der Karteninhaber zu seinem Fahrzeug zurückkehrt, entfernt der Kriminelle das Gerät und entnimmt die Karte. Kopierte Tankkarten werden in der Regel an unbemannten Tankstellen oder an automatischen Zahlungsterminals bemannter Tankstellen eingesetzt – sehr häufig zu Randzeiten, d.h. nachts oder am Wochenende. Auch lässt sich feststellen, dass kopierte/geskimmte Karten meist nicht dort eingesetzt werden, wo sie kopiert wurden.

Technisch weniger avancierte Formen des Missbrauchs von Karten sind zum Beispiel das „Schulter-Surfen“, bei dem Kriminelle heimlich beobachten, wie ein Nutzer seine PIN eingibt, oder der Einbruch in ein geparktes Fahrzeug, um Kartendaten zu kopieren. Tankkarten-Kriminelle wissen, dass Lkw-Fahrer häufig Post-it-Notizen mit den Karten- und PIN-Angaben im Fahrzeug mit sich führen. Sobald sie diese Informationen gefunden und kopiert haben, verlassen die Kriminellen das Fahrzeug, oft ohne Spuren zu hinterlassen. Betroffene Fahrer bemerken so erst gar nicht, dass ihre Karten kompromittiert wurden.

Karten mit Chip und PIN bieten zwar einen gewissen Schutz vor Skimming, doch dieser Vorteil wird dadurch hinfällig, dass bei einer Beschädigung des Chips doch der Magnetstreifen genutzt wird. Tankkarten-Betrüger zerstören also einfach den Chip der Karte, indem sie ihn zerkratzen, mit einem Aufkleber abdecken ihn einfach mit einem Hammer aus der Karte herausschlagen.

Skimming und kopierte Karten sind die häufigsten Formen des Tankkartenbetrugs.

2 Laut ai Corp waren 97 % der Fälle in Italien im Jahr 2019 Betrugsfälle durch Skimming.

02

Neben Skimming und dem Kopieren von Karten existieren die folgenden häufigen Formen des Tankkartenbetrugs:

Betrug mit verlorenen und gestohlenen Karten

Hierbei stehlen Kriminelle Karten und gegebenenfalls PIN-Nummern. Auch ohne PIN können gestohlene Karten in Systemen, die keine PIN erfordern (zum Beispiel Online-Shops), betrügerisch verwendet werden. Die meisten Betrugsfälle dieser Form beziehen sich auf Einkäufe mit Karten, die getätigt wurden, bevor der Verlust der Karten festgestellt oder gemeldet worden war, oder bei denen es zu Verzögerungen bei der Kartensperrung kam.

Absprachen am Standort

Bei diesem Betrugstyp treffen Fahrer mit dem Tankstellenpersonal Absprachen und zahlen für Kraftstoff, der nicht getankt wurde, oder zahlen für den Kraftstoff mehr als eigentlich berechnet wurde. Der Tankwert wird häufig gegen Bargeld oder Waren wie beispielsweise Zigaretten getauscht. Dies wird manchmal als „Dieselization“ bezeichnet. Das Wissen um Standorte, die offen für derartige Absprachen sind, wird oft von Fahrer zu Fahrer weitergegeben.

Missbräuchliche Nutzung einer echten Karte durch den Karteninhaber (Fahrerbetrug)

Dabei wird eine Tankkarte für andere Zwecke verwendet als die, für die sie vorgesehen ist. Zum Beispiel der Kauf von Kraftstoff für ein anderes Fahrzeug oder einen anderen Fahrer gegen Bargeld; der Kauf von Kraftstoff, der dann wieder aus dem Tank abgesaugt wird; die Betankung eines versteckten Extratanks; die Beschädigung von Chip oder Magnetstreifen einer Karte, um Kaufüberprüfungen zu umgehen oder um den Kauf von Treibstoff mit Bargeld zu rechtfertigen, um den Kauf von nicht genehmigten Waren zu verschleiern; dazu zählen auch Fälle, in denen Fahrer die Daten von Karten früherer Arbeitgeber nutzen. Betrug durch den Fahrer ist besonders schwer festzustellen, da hierbei scheinbar ganz normales Kaufverhalten des Fahrers bzw. standard-mäßige Kartennutzung vorzuliegen scheint.

Interner Betrug

Hier handeln Mitarbeiter oder Auftragnehmer allein oder in Absprache mit externen Parteien (freiwillig oder aufgrund von Zwang oder Bestechung), um geschäftlich sensible Daten, Informationen oder Materialien zu stehlen und sie eventuell dazu zu verwenden, den Betrieb oder die Sicherheit eines Unternehmens zu gefährden.

02

Betrug durch Abfangen von Karten auf dem Postweg

Dies beinhaltet das Abfangen von Karten und/oder PINs an der Adresse eines Kunden, in einem Postsortierzentrum oder innerhalb des Postverteilungssystems. Kompromittierte Karten werden kopiert, wieder in den Umschlag gelegt und in die Post gegeben und an den Kunden ausgeliefert. Besonders gefährdet sind hierbei Unternehmen mit einer Briefkastenanlage oder Unternehmen, denen bei einem Umzug die Post nicht nachgesendet wird. Es sind auch Fälle bekannt, in denen Karten und PIN-Nummern in Postsortierzentren an Flughäfen und anderen Orten abgefangen wurden.

Identitäts- und Antragsbetrug

Hierbei geben sich Kriminelle als ein Unternehmen aus oder übernehmen tatsächlich ein Unternehmen, um ein Konto mit gefälschten oder gestohlenen Unterlagen zu eröffnen. Wenn ein gefälschter Antrag erfolgreich ist, werden an die Betrüger Karten ausgegeben und diese werden dann genutzt. Zwar werden die bezogenen Leistungen vom Tankkartenanbieter in Rechnung gestellt, doch bis zur Fälligkeit der Rechnungen bzw. bis der Betrug auffällt, hatten Kriminelle dann bereits mehr als genug Zeit für betrügerische Aktivitäten. Diese Form des Tankkartenbetrugs fällt häufig erst dadurch auf, dass Rechnungen auch nach mehrfachen Mahnungen nicht bezahlt werden.

Betrug mit „Card not present"-Transaktionen

Dies bezieht sich auf den Diebstahl von Kartendaten, die dann für Online-Käufe verwendet werden, was von den echten Karteninhabern erst bemerkt wird, wenn sie ihren Kontoauszug prüfen. Kriminelle gelangen an Tankkartennummern mittels spezieller Software, die gültige Kartennummern generiert oder mittels Skimming und Datenspionage. Sie verkaufen diese Karten dann an Fahrer, die diese in Mautnetzwerken verwenden. Kriminelle nutzen Online-Portale, um Fährtickets, Eurovignetten und Mauttickets mit den Kartendaten eines Unternehmens (üblicherweise eines früheren Arbeitgebers) für die Fahrzeuge eines anderen Unternehmens zu bestellen (typischerweise der aktuelle Arbeitgeber oder auch ein unabhängiger Einzelunternehmer, mit dem eine entsprechende Absprache getroffen wurde.)

Fahrzeug-Cloning

Bei diesem Betrugstyp wird das Kennzeichen eines Fahrzeugs kopiert und für ein anderes Fahrzeug derselben Automarke und desselben Modells verwendet, um so Kraftstoffkosten, Maut- und Parkgebühren zu erschleichen.

02 Das Profil eines Betrügers

Die folgenden Eigenschaften sind typisch für Betrüger[3]:

69% sind zwischen **36 und 55** Jahre alt

79% sind **männlich** (jedoch steigt der Anteil von Frauen)

62% haben wahrscheinlich **Absprachen** mit anderen **getroffen**

65% sind Mitarbeiter, die ihren **eigenen Arbeitgeber** betrügen

35% sind Mitglieder der **Geschäftsleitung** (einschließlich Vorstandsmitglieder)

38% arbeiteten mindestens **sechs Jahre** bei ihrem Unternehmen, bevor sie Betrug begingen

An großangelegtem Betrug sind in der Regel Führungskräfte beteiligt, die aufgrund ihrer Autoritätsebene interne Kontrollen umgehen können.

Weitere typische Eigenschaften von Betrugskriminellen:

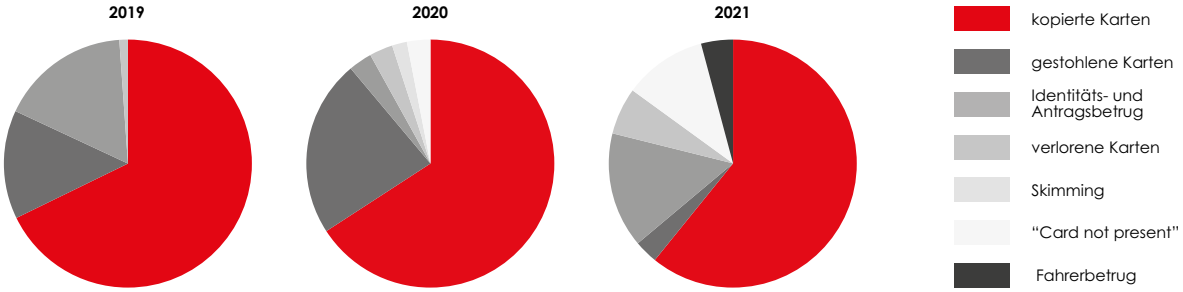
- sie nehmen keinen Urlaub
- sie geben keine Einblicke in Geschäftsvorgänge
- sie lehnen Kontrollen ab
- sie haben geringe interpersonelle Kompetenzen
- sie haben gute technische Fähigkeiten
- sie arbeiten bis spät in den Abend
- sie neigen zu Drogen- / Alkoholmissbrauch
- sie tendieren zu Beziehungsproblemen

3 Quelle: KPMG Global Profiles of the Fraudster, 2016

02

Beispiele für die Entwicklung von Tankkartenbetrug in Europa 2019 - 2021

Anteil der verschiedenen Betrugstypen am finanziellen Gesamtschaden durch Betrug pro Jahr



Die Formen von Tankkartenbetrug wandeln sich fortlaufend und entwickeln sich weiter. Um einen kontinuierlich hohen Sicherheitsstandard bieten zu können, sind daher eine regelmäßige Risikobewertung und die stetige Weiterentwicklung von Präventions- und Betrugserkennungsmaßnahmen unerlässlich.

Kartenbetrug entwickelt sich:

- von einzelnen Kriminellen zu organisierten und internationalen Verbrecherbanden
- vom Skimming einer einzelnen Karte zu Angriffen auf die Datensicherheit insgesamt
- von Kriminellen, die den ganzen Betrugszyklus abdecken, zu Betrügern, die sich auf einen Teil dieser „Wertschöpfungskette" spezialisieren und diesen Wert an die nächste Stufe weiterverkaufen

Kriminelle wenden immer ausgefeiltere Methoden an:

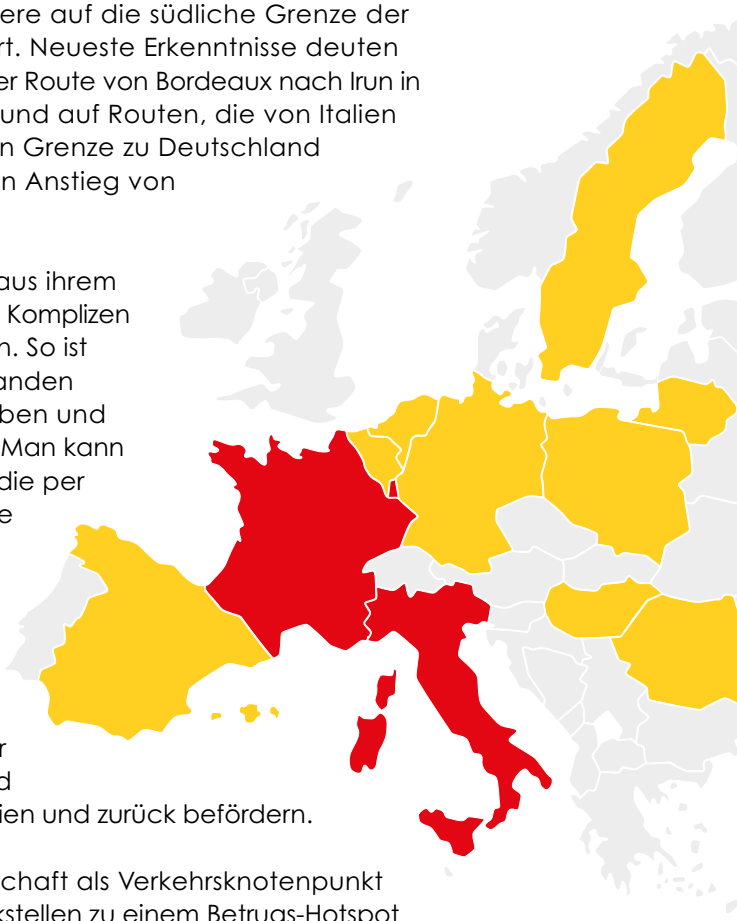
- Geräte-Manipulation („Device Spoofing")
- Standort-Manipulation
- Bots
- Annahme gefälschter digitaler Identitäten
- Tarnung als Kunde
- „Fraud-as-a-Service" (FaaS), d.h. Betrug als „Dienstleistung", häufig über das Dark Web angeboten von global operierenden Verbrecherbanden und allein arbeitenden Betrügern

03 Regionale Schwerpunkte von Tankkartenbetrug in Europa

Im heutigen digitalen Zeitalter werden Betrugstechniken mit jedem Tag ausgeklügelter. In der Vergangenheit stellten Kriminelle üblicherweise eine einzige Kopie einer Tankkarte her, aber heutzutage werden häufig gleich mehrere Kopien angefertigt und an Komplizen in verschiedenen Ländern verteilt, um so größtmöglichen finanziellen Gewinn zu erzielen. Dafür müssen sich die Kriminellen organisieren. Und in der Tat sind viele in – oft länder-übergreifenden – Banden organisiert, die neben Tankkartenbetrug häufig auch in Drogen-, Menschen- oder Waffenhandel verwickelt sind.

Organisierte Banden existieren überall in Europa[4], und viele haben einen geografischen Schwerpunkt für ihre kriminellen Aktivitäten ausgewählt. Daten zeigen, dass sich eine Bande auf Autobahntankstellen an größeren Ost-West- oder Nord-Süd-Knotenpunkten in Frankreich konzentriert, während sich eine andere auf die südliche Grenze der Niederlande zu Belgien und Deutschland fokussiert. Neueste Erkenntnisse deuten auf deutlich erhöhte kriminelle Aktivitäten entlang der Route von Bordeaux nach Irun in Spanien hin, zudem an der italienischen Ostküste und auf Routen, die von Italien nach Slowenien führen. Auch an der französischen Grenze zu Deutschland und der Schweiz wurde in den letzten Monaten ein Anstieg von Tankkartenbetrugsfällen festgestellt.

Es gibt auch kriminelle Banden, die es auf Fahrer aus ihrem Heimatland abgesehen haben - Länder, in denen sie Komplizen haben, die bei der Durchführung des Betrugs helfen. So ist zu vermuten, dass in Frankreich und in den Niederlanden aktive Banden Verbindungen nach Osteuropa haben und es auf Fahrer aus dieser Region abgesehen haben. Man kann davon ausgehen, dass die meisten Eurovignetten, die per Onlinekriminalität erworben werden, für Fahrzeuge gedacht sind, die in Osteuropa ansässigen Unternehmen gehören.



Betrugs-Hotspots
2019-2021

Generell lässt sich sagen, dass die geografische Verteilung von Betrugsdelikten die Fahrtstrecken von Transportunternehmen widerspiegelt, die in Osteuropa ihren Sitz haben und Waren in westlicher und südlicher Richtung durch Italien, Frankreich und Spanien und in nördlicher Richtung nach Skandinavien und zurück befördern.

Insbesondere Frankreich ist aufgrund seiner Eigenschaft als Verkehrsknotenpunkt und aufgrund seiner zahlreichen unbemannten Tankstellen zu einem Betrugs-Hotspot geworden. Die meisten Skimming-Betrugsfälle finden an unbemannten Tankstellen nördlich und östlich von Paris und in den Hauptverkehrsknotenpunkten rund um Lyon und Grenoble statt. Weiter südlich verzeichnete Perpignan im ersten Quartal 2021 einen signifikanten Anstieg der Kriminalitätsrate.

Tankstellen und Rastplätze entlang der Grenze zwischen Frankreich und Spanien und in der holländischen Grenzregion um Venlo sind die Hauptorte für Fahrzeugeinbrüche und den missbräuchlichen Einsatz von kopierten Karten.

Die fortlaufende Überwachung der Betrugsstatistik und der geografischen Verteilung von Tankkartenkriminalität hilft bei der Prävention von kriminellen Angriffen und ist zudem die Voraussetzung dafür, im Betrugsfall schnell eingreifen zu können.

4 Quelle Europol: In den Niederlanden verursachte ein massiver Copy Card-Vorfall mit zahlreichen betroffenen Karten einen finanziellen Schaden von 800.000 US-Dollar innerhalb weniger Wochen. In Italien entstand bei einem Betrugsvorfall ein Verlust von 3,2 Mio. US-Dollar in weniger als zwei Monaten. 2018 hob Europol eine spanische Verbrecherbande aus, die gefälschte Tankkarten im spanischen und französischen Mautsystem einsetzte: Dabei wurden 24 Personen verhaftet, 600 Kraftfahrzeugkennzeichen waren manipuliert, 11 Herstellungsanlagen für gefälschte Tankkarten wurden aufgelöst, 15.000 gefälschte Karten beschlagnahmt. Insgesamt belief sich der verursachte finanzielle Schaden auf 500.000 Euro.

04 Strategien zur Prävention von Tankkartenbetrug

Was kann getan werden, um das Risiko von Kartenbetrug zu verringern und den sich ständig weiterentwickelnden Strategien und Taktiken von Kriminellen entgegenzutreten? Der Schlüssel zum Erfolg liegt in der engen Zusammenarbeit von Kartenanbietern, Partnerunternehmen, Flottenmanagern und Fahrern. Im gemeinsamen Bemühen lässt sich am effektivsten ein hohes Sicherheitsniveau erreichen und aufrechterhalten.

4.1 Maßnahmen für Tankkartenanbieter

Da sich der Betrug mit Tankkarten zu einer europaweiten Bedrohung durch internationale Banden entwickelt hat, erfordern die Ermittlungen und Strafverfolgung die Zusammenarbeit mit internationalen Einrichtungen und Behörden. Zwei wichtige Institutionen auf diesem Gebiet sind zum einen das Fuel Industry Card Fraud Investigation Bureau (FICFIB), ein Zusammenschluss von Kartenherausgebern, Kraftstoffhändlern und unabhängigen Tankstellenbetreibern, die Informationen über Trends, Schwachpunkte und sich entwickelnde Bedrohungen austauschen, und zum anderen Europol, die Informationen zu grenzüberschreitenden Vorfällen mit den jeweils lokalen Polizeibehörden teilt und so die Ermittlungsarbeiten beschleunigt. Die enge Zusammenarbeit mit diesen Organisationen gibt Kartenanbietern die internationale Schlagkraft, die sie für erfolgreiche Maßnahmen bei Betrugsfällen benötigen.

Zusätzlich zur Kooperation mit Behörden und Institutionen ist es für Tankkartenanbieter äußerst wichtig, die eigenen Produkte, Dienstleistungen, Systeme und Prozesse fortlaufend zu überwachen, auf Schwachstellen zu prüfen und kontinuierlich zu optimieren. Dies beginnt schon bei der Planung von Produkten, Dienstleistungen und Services (z.B. Transaction Notification) und beinhaltet auch die regelmäßige Schulung und Weiterbildung des Kundenservice und die stetige Qualitätssicherung von IT-Prozessen, um sicherzustellen, dass kriminellen Aktivitäten so schnell wie möglich entgegengewirkt werden kann.

Nicht zuletzt ist Kommunikation ein essentieller Bestandteil des Themas Kartensicherheit. Kommunikationsprozesse mit Behörden, Partnern und Kunden müssen schnell und fokussiert sein. Im Betrugsfall ist eine schnelle Kommunikation mit Betroffenen von großer Bedeutung. Des Weiteren ist es wichtig, das Bewusstsein von Kunden und Partnern in Bezug auf die Gefahren des Tankkartenbetrugs zu schärfen und sie bei der Prävention zu unterstützen.

04

4.2 UTAs Ansatz zur Prävention von Kartenbetrug

Für einen Mobilitätsdienstleister sind Tank- und Servicekarten Eckpfeiler des Produkt- und Dienstleistungsportfolios. Dementsprechend besitzt das Thema Karten- und Transaktionssicherheit bei UTA höchste Priorität.

Im Mittelpunkt der Betrugspräventionsmaßnahmen von UTA steht das eigene Betrugs- und Kartensicherheitsteam mit den folgenden Tätigkeitsfeldern und Services:

- Echtzeit Transaction Notifications, durch die Kunden schnell auf verdächtige Transaktionen reagieren können
- Telefonischer Hinweisservice bei verdächtigen Vorkommnissen
- Entwicklung und Umsetzung von Strategien und Prozessen für die wirksame Erkennung, Bekämpfung und Prävention von Betrug
- Bewertung und Empfehlung von technischen Systemen, um das Betrugsrisiko zu reduzieren
- Zusammenarbeit mit Rechtsanwälten, Strafverfolgungsbehörden, dem FICFIB und anderen Institutionen, um Konzepte und Prozesse für die Aufklärung von Betrugsfällen zu entwickeln und umzusetzen
- Informationsrecherche und Erstellung von Berichten, um polizeiliche Ermittlungen zu unterstützen
- Befragung von Betrugsopfern und Verdächtigen, um Informationen zur Art der Angriffe einzuholen

"Mit unseren Produkten, Dienstleistungen und Prozessen setzen wir uns dafür ein, unsere Kunden sowohl vor aktuell bekannten als auch vor neuen Formen des Tankkartenbetrugs zu schützen."

Carsten Bettermann,
CEO von UTA

Die Sicherheit von Tankkarten und Transaktionen ist der entscheidende Erfolgsfaktor für Mobilitätsdienstleister.

04

Nutzung von Brancheninformationen

Neben dem eigenen Betrugspräventionsteam ist ein weiterer Grund für UTAs hohe Aufklärungsrate von Betrugsfällen das umfassende Fachwissen, das das Unternehmen in Jahren der Zusammenarbeit mit führenden Sicherheitsorganisationen, Industrieverbänden und externen Experten erworben hat.

In Bereichen, in denen UTA nicht auf ausreichendes internes Fachwissen zurückgreifen kann, geht das Unternehmen Partnerschaften mit Spezialisten ein. Beispiele hierfür sind der Bereich Cyber-Forensik, die Absicherung der Prozesse rund um Zahlungskarten und Bankprodukte, Recherchen im Web oder umfangreiche kriminalpolizeiliche Ermittlungen. Für die algorithmenbasierte, automatisierte und optimierte Betrugserkennung arbeitet UTA beispielsweise mit The ai Corporation Ltd. zusammen, einem Spezialisten für auf Künstliche Intelligenz (KI) gestützte Systeme zur Zahlungssicherheit und Transaktionsüberwachung. UTA ist Mitglied des FICFIB, kooperiert eng mit Europol und ist zudem aktives Mitglied von Industrieverbänden, die gemeinsame Standards für den sicheren Austausch von Daten zwischen Kartenakzeptanz-Netzwerken und Kartenherausgebern festlegen.

Daneben arbeitet UTA mit Tankstellenbetreibern in 40 europäischen Ländern zusammen, um sicherzustellen, dass vor Ort die erforderlichen Sicherheitsmaßnahmen entsprechend umgesetzt werden. Dazu zählen zum Beispiel die Installation von Videoüberwachungssystemen oder IP-Kameras, Schutzmaßnahmen, die den Einbau von Skimming-Vorrichtungen verhindern sowie die Einrichtung von Online-Transaktionsgenehmigungen.

Als Teil der weltweit tätigen Edenred-Gruppe profitiert UTA vom Fachwissen des Mutterkonzerns auf Gebieten wie Compliance, Datenschutz und IT-Sicherheit. Das langjährige Fraud Forum (Betrugsforum) von Edenred deckt sämtliche Geschäftsfelder des Konzerns in mehr als 50 Ländern ab und teilt fortlaufend Erkenntnisse und Best Practices zu Sicherheitsthemen.

"Künstliche Intelligenz und maschinelles Lernen sind heute unverzichtbare Werkzeuge, um Tankkartenbetrug effektiv zu verhindern und Betrugsfälle zu erkennen. In unserer Kooperation mit UTA kombinieren wir modernste technische Systeme (aiAutoPilotML) und das Know-how unserer Tankkartenexperten mit der umfassenden Expertise von UTA im Bereich der Prävention und Erkennung von Tankkartenbetrug. Durch diese Bündelung von Technologie, Erfahrung und Expertenwissen erreichen wir eine sehr hohe Schlagkraft und Erfolgsquote bei der Prävention und Bekämpfung von Kartenbetrug."

Dr. Mark Goldspink,
CEO von The ai Corporation Ltd

Internes Fachwissen kombiniert mit der Expertise spezialisierter Partner ermöglicht optimale Ergebnisse.

04 Proaktiver und präventiver Ansatz

Um sicherzustellen, dass ihre Systemplattformen und Produkte von Grund auf höchste Sicherheit bieten, verfolgt UTA einen „Security by design"-Ansatz. Das Unternehmen investiert dazu erheblich in Forschung und Entwicklung in Bereichen wie Datenanalytik, künstliche Intelligenz und maschinelles Lernen, um dem Betrugs- und Kartensicherheitsteam die geeigneten Werkzeuge für die noch bessere Erkennung der sich immer schneller wandelnden Betrugsarten an die Hand zu geben. So hat UTA beispielweise zur Bekämpfung von massenhaften Kartenfälschungen geografische Plausibilitätskontrollen eingeführt, die die Zeit und Entfernung zwischen Transaktionsorten nachverfolgen und prüfen. So kann evaluiert werden, ob der Einsatz ein und derselben Karte für die betreffenden Transaktionen überhaupt möglich ist oder ob es sich dabei um den Einsatz von Kartenkopien handeln muss. Im Betrugsfall können Karten so umgehend gesperrt und die betroffenen Kunden schnell informiert werden.

Der detaillierte Überblick von UTAs Kartensicherheitsteam über das weite Feld des Tankkartenbetrugs in Europa und sein weitreichendes Netzwerk mit Institutionen und Organisationen hilft, das Kundenrisiko zu minimieren, bei Bedarf die Unterstützung von Europol und anderer Sicherheitsbehörden in Anspruch zu nehmen, Informationen innerhalb des FICFIB zu teilen und so die Aufklärung und Verfolgung von Betrugsfällen zu beschleunigen.

„Wir arbeiten intensiv an der Entwicklung einer digitalen Tankkarte. Bei dieser Lösung werden UTAs Expertise rund um Transaktionssicherheit und Betrugsprävention und das Know-how unseres Mutterkonzerns Edenred im Bereich Zahlungsdienstleistungen erfolgreich zusammengeführt."

Carsten Bettermann,
CEO von UTA

Digitale Tankkarten – Schneller, komfortabler und sicherer

Kontaktlose, digitale Abwicklungsverfahren sind auf dem Vormarsch – ein Trend, der durch die Corona-Pandemie noch beschleunigt wurde. Digitale Tankkarten, die als App auf dem Smartphone genutzt werden, erlauben nicht nur die einfache Abwicklung des Kraftstoffbezugs direkt an der Zapfsäule, sondern sorgen generell für schnellere und komfortablere Prozesse, von der Anmeldung und Registrierung im System bis hin zur Verwaltung der eigenen Daten und Buchungen. Ihr weiterer großer Vorteil liegt in der zusätzlichen Sicherheit, die sie dem Nutzer bei seinen Transaktionen gegenüber physischen Tankkarten bieten.

04 Minimierung des Kundenrisikos

Um für Kunden das Kartenbetrugsrisiko zu reduzieren, hat UTA eine Reihe von Sicherheitsfunktionen und -services eingeführt. Diese umfassen das Sperren von Karten über das rund um die Uhr verfügbare Online-Portal von UTA, PIN-Nummern für alle Karten, die Festlegung individueller Transaktionslimits, die Kontrolle über Ort und Zeit von Transaktionen sowie transparente Rechnungsstellung und übersichtliches Berichtswesen.

Der Transaktionsbenachrichtigungsservice (UTA Transaction Notification) von UTA benachrichtigt Kunden in Echtzeit, wenn Transaktionen mit Tankkarten von UTA erfolgen. So kann sofort eingegriffen werden, wenn verdächtige Aktivitäten festgestellt werden. Dieser Service kann sehr individuell auf die Bedürfnisse jedes Kunden zugeschnitten werden; beispielsweise lassen sich Filter setzen, um Benachrichtigungen via Textnachricht oder E-Mail zu erhalten, um einen Grenzwert pro Transaktion festzulegen, ab dem eine Warnmeldung ausgegeben wird, oder auch um länderspezifische Datums- oder Uhrzeitbeschränkungen festzulegen.

Sollte trotz aller Sicherheitsvorkehrungen doch ein Kunde Opfer von Betrug werden, so leistet UTA wo immer es möglich ist Unterstützung. So kontaktiert das Unternehmen zum Beispiel Tankstellenbetreiber und bittet um Sicherstellung von Videobeweismaterial und das Betrugs- und Kartensicherheitsteam kooperiert mit der Polizei und relevanten Behörden, um sachdienliche Informationen weiterzugeben und so die Ermittlungsarbeit zu unterstützen.

UTAs Präventions- und Sicherheitskonzept – Eine Erfolgsgeschichte

UTAs Sicherheitsansatz besteht im Wesentlichen darin, kriminelle Aktivitäten frühzeitig zu erkennen, zu lokalisieren und zu unterbinden, bevor Kunden geschädigt werden. Der Erfolg bestätigt diese Strategie. Das Unternehmen erkennt nahezu 90 % aller Betrugsfälle, bevor sie von den Kunden selbst festgestellt werden. Vor zwei Jahren betrug diese Quote bei UTA noch 63 %. Die signifikante Verbesserung von UTAs Anti-Betrugs-Quote unterstreicht die Wirksamkeit der implementierten Maßnahmen und Systeme. UTA erkennt nicht nur einen sehr großen Teil von Betrugsfällen, sondern identifiziert sie auch deutlich schneller. So konnte der Mobilitätsdienstleister die durch-schnittlichen Verluste durch Betrug in den letzten Jahren stark reduzieren.

04

4.3 Best Practices für Tankkartennutzer

Bei allen Bemühungen der Kartenherausgeber, ihre Kunden zu schützen, müssen auch die Tankkartennutzer selbst aktiv mitarbeiten, indem sie sicherstellen, dass ihre Karten sicher aufbewahrt werden und Missbrauch aktiv vorgebeugt wird.

Folgende Tipps sollten Tankkarten nutzende Unternehmen berücksichtigen:

Tipps für Fahrer:

PIN-Sicherheit
Kartennutzer sollten sich ihre PIN-Nummer merken und diese niemals notieren und zusammen mit der betreffenden Karte aufbewahren. PIN-Nummern sollten weder als Geburtsdatum oder Telefonnummer auf einem mobilen Gerät gespeichert werden, noch sollten sie einer anderen Person mitgeteilt werden. Darüber hinaus sollten Nutzer ihre Hand bei Eingabe ihrer PIN in ein Zahlungsgerät als Sichtschutz einsetzen.

Kartensicherheit
Fahrer sollten ihre Karte niemals unbeaufsichtigt in der Kabine ihres Fahrzeugs oder auf dem Firmengelände lassen. Jede unbeaufsichtigte Karte läuft Gefahr, unbemerkt kopiert zu werden.

Wachsam bleiben
Kartennutzer sollten Zapfsäulen stets auf Anzeichen für Manipulationen überprüfen und alles melden, was ihnen verdächtig vorkommt. Am sichersten ist es, Zapfsäulen zu nutzen, die sich nahe am Kassenhäuschen und in Sichtweite des Kassierers bzw. der Kassiererin und/oder der Videoüberwachung befinden. Bei der Zahlung im Shop/Kassenhäuschen, sollte die Karte möglichst nicht dem Angestellten übergeben, sondern stattdessen vom Fahrer selbst in das Kartenlesegerät eingeführt werden. Auch sollte man stets wachsam sein und einen Blick auf verdächtige Fahrzeuge haben, die in der Nähe parken.

Tipps für Flottenmanager:

Melden von verdächtigem Verhalten oder verdächtigen Vorkommnissen
Arbeitgeber sollten unverzüglich Anzeige bei der Polizei erstatten, wenn ihre Fahrer von Tankstellenpersonal oder anderen Personen angesprochen und zu betrügerischen Handlungen verleitet werden. Der Verlust oder Diebstahl von Karten sowie jeder Vorfall, bei dem PIN-Nummern kompromittiert wurden, sollte umgehend gemeldet werden. Dabei ist es wichtig, Vorfälle sowohl der Polizei im Land der Tat zu melden, als auch im Land des Unternehmenssitzes. Dies kann die grenzüberschreitende Zusammenarbeit zwischen den Polizeibehörden beschleunigen und so zu einem schnelleren Ermittlungsergebnis führen.

04

Prüfung von Transaktionen
Arbeitgeber sollten Rechnungen und Belege umgehend prüfen, um sicherzustellen, dass alle Zahlungen in Ordnung sind. Darüber hinaus sollten die Verbrauchsberichte für Fahrzeuge überwacht werden, um Fälle von übermäßigem Treibstoffverbrauch festzustellen.

Aufklärung und Sensibilisierung der Fahrer
Arbeitgeber sollten ihre Fahrer hinsichtlich ihrer persönlichen Verantwortung aufklären und ihnen vermitteln, dass der Missbrauch von Tankkarten kein Kavaliersdelikt, sondern eine Straftat ist, die zum Verlust des Arbeitsplatzes und/oder strafrechtlicher Verfolgung führen kann. Darüber hinaus empfiehlt es sich für Arbeitgeber, sich von ihren Fahrern per schriftlicher Vereinbarung bestätigen zu lassen, dass sie über die möglichen Folgen von Fehlverhalten beim Umgang mit Tankkarten und dem Führen von Firmenfahrzeugen informiert wurden und diese Informationen verstanden haben.

Kartenkontrollen
Arbeitgeber haben die Möglichkeit Obergrenzen für Transaktionssummen pro Karte festzulegen und auch die Häufigkeit des Karteneinsatzes auf täglicher oder monatlicher Basis zu begrenzen. Außerdem kann festgelegt werden, welche Produkte oder Dienstleistungen über die Tankkarte bezogen werden können. Diese Nutzungseinschränkungen sind effektive Maßnahmen für die Betrugsprävention und sollten unbedingt genutzt werden.

„Sanfte“ Kontrollen
Ungefähr 43 % der Betrugsvorfälle werden aufgrund von Whistleblowern oder anderen Hinweisen entdeckt[5]. Die Einführung eines Whistleblowing-Systems kann auch wirtschaftliche Vorteile für Unternehmen haben: Mitarbeiter und andere Personen mit Firmenbezug sind sozusagen die erste und effektivste Verteidigungslinie gegen kriminelle Übergriffe. Über solche Früherkennungsmaßnahmen erhalten Unternehmen die Möglichkeit, schnell und frühzeitig zu reagieren und so finanzielle Schäden und Reputationsverlust zu verhindern. Häufig sind höher positionierte Mitarbeiter und sogar Führungskräfte an Betrugsaktivitäten beteiligt, weil sie interne Kontrollen aufgrund ihrer hohen Autoritätsebene umgehen können. Prävention erfordert ein Arbeitsumfeld, das ethisches Verhalten fördert, Fehlverhalten unterbindet und Mitarbeiter ermutigt, bekanntes oder vermutetes Fehlverhalten zu melden. Potentielle Betrüger werden an der Umsetzung krimineller Aktivitäten gehindert, wenn sie keine Unterstützung durch andere Mitarbeiter erhalten. Auch wenn solche „sanfte“ Kontrollen zur Förderung eines angemessenen Arbeitsplatzverhaltens eher langfristige Maßnahmen und schwieriger durchzuführen sind als „harte“ Kontrollen, so sind sie dennoch die beste nachhaltige Vorbeugung gegen Betrug.

5 Quelle: KPMG

05

Richtig Anzeige erstatten bei Tankartenbetrug

Antworten auf die häufigsten Fragen

Im Fall eines vermuteten oder bestätigten Betrugsfalls sollte folgendes beachtet werden:

An wen sollte man sich im Falle eines Betrugs zuerst wenden?

Wenden Sie sich bitte sofort an UTA, wenn Ihnen eine Transaktion über die UTA-Karte verdächtig erscheint oder Sie die Transaktion nicht ausgeführt haben. Sie können Ihre Karte unter der Telefonnummer 00 800 88 22 62 26 oder über den UTA Exklusiv-bereich sperren lassen. Danach sollten Sie bei der lokalen Polizei Anzeige erstatten.

Warum sollte ich bei der Polizei Anzeige erstatten?

Betrug und der Missbrauch von Karten für nicht genehmigte Transaktionen sind Straftaten. Denken Sie daran, dass Sie möglicherweise nicht das einzige Opfer sind, und dass der Täter eventuell noch andere schwere Verbrechen begangen haben könnte. Um diese Betrüger strafrechtlich zu verfolgen, müssen Sie jeden Betrugs- oder Missbrauchsfall der Polizei melden. Nur so kann der polizeiliche Ermittlungsapparat effektiv tätig werden.

Wann sollte ich Anzeige erstatten?

Sie sollten sich unverzüglich nach Feststellen eines Betrugsvorfalls an die Polizei wenden, da das Verbrechen eventuell noch im Gange ist. Beweise, die für die Polizei nützlich sein können, wie zum Beispiel Videoaufnahmen, werden gewöhnlich nur für einen begrenzten Zeitraum aufbewahrt. Der Auf-bewahrungszeitraum hängt von den rechtlichen Bestimmungen des Landes ab, in dem das Verbrechen begangen wurde. Es zählt also Schnelligkeit bei der Meldung und Verfolgung von kriminellen Handlungen.

In welchem Land sollte ich den Vorfall melden?

Wenn Sie international tätig sind, sollten Sie den Vorfall der Polizei in dem Land anzeigen, in dem sich der Vorfall ereignete, und auch in Ihrem Heimatland Meldung machen. Im Falle eines grenzübergreifenden Betrugs müssen Polizei-beamte verschiedener Länder eventuell für Ermittlungen und strafrechtliche Verfolgungen miteinander kooperieren, was durch Ihre Meldung in beiden Ländern erleichtert und beschleunigt wird.

Welche Angaben sollte ich machen?

Jede Ermittlung ist anders, aber die folgenden Angaben sollten gegenüber der Polizei gemacht werden können:

- Angaben zum Unternehmen, einschließlich Anschrift und Umsatzsteuernummer
- Eine Beschreibung des Vorfalls, einschließlich der betroffenen Kartennummer(n) / Bank Identification Number (BIN), Ort, Datum und Uhrzeit, Höhe des Diebstahlschadens
- Angaben, wo die Karte und die PIN-Nummer gewöhnlich aufbewahrt werden
- Ob Sie noch immer im Besitz der Karte sind
- Ob die Karte gesperrt wurde, und falls ja, wann
- Wo Ihre Fahrer kurz vor dem Vorfall waren, zum Beispiel beim Tanken, auf dem Parkplatz etc.
- Jede weitere relevante Information …

06 Fazit

Information, Wachsamkeit, Monitoring, die richtigen technischen Systeme und schnelle Reaktionen im Ernstfall – So bleibt Tankkartenbetrügern kaum eine Chance.

Tankkartenbetrug ist eine ständig wachsende Gefahr, die Unternehmen erhebliche finanzielle Verluste zufügen kann. Genaue Kenntnis der Betrugstaktiken und ihrer regionalen Verbreitung, konsequente Kontrolle von Transaktionen und Abrechnungen sowie die Schulung und Sensibilisierung von Fahrern sind für Fuhrparkmanager die wichtigsten Schritte hin zu mehr Sicherheit für ihre Flotte.

Der Einsatz technischer Tools und die Implementierung relevanter Sicherheitssysteme sorgen darüber hinaus für bessere Prävention, effektivere Früherkennung und schnellere Reaktion auf Betrugsfälle. Der beste Schutz vor Tankkartenbetrug ergibt sich daher aus dem engen, partnerschaftlichen Zusammenspiel von Fuhrparkbetreiber bzw. Flottenmanager und qualifiziertem Tankkartenanbieter.

Bei UTA stehen die Sicherheit und der Schutz der Kunden an erster Stelle. Das Unternehmen wird sich auch weiterhin intensiv dafür engagieren, alle Formen von Tankkartenbetrug einzudämmen und die Risiken für seine Kunden zu minimieren.

Für weitere Informationen

Für weitere Informationen zum Betrug mit Tankkarten oder wenn Sie mehr über die Sicherheitsverfahren und Techniklösungen von UTA erfahren möchten, wenden Sie sich bitte an:

Steffen Glaab

Head of Fraud & Prevention Management

steffen.glaab@uta.com

Über UTA

Die **UNION TANK Eckstein GmbH & Co. KG (UTA)** ist ein führender Anbieter von Tank- und Servicekarten in Europa. Gewerbliche Kunden können mit dem UTA-Kartensystem an über 68.000 Annahmestellen in 40 europäischen Ländern markenunabhängig und bargeldlos tanken. Die UTA-Karte kann ferner für die Mautabrechnung, Reparaturen sowie Pannen- und Abschleppdienste verwendet werden. Darüber hinaus können Rückerstattungen der Mehrwert-und Mineralölsteuer über einen Service-Provider-Partner von UTA in Anspruch genommen werden. In einer Umfrage, die vom deutschen Magazin Wirtschaftswoche und dem Kölner Marktforschungsinstitut ServiceValue durchgeführt wurde, wurde UTA zum „Besten Tankkarten-Dienstleister für den Mittelstand 2021" gewählt. Das 1963 von Heinrich Eckstein gegründete Unternehmen UTA befindet sich heute im Besitz der Edenred SE.

Für mehr Informationen: www.uta.com

Über Edenred

Edenred begleitet mit seiner führenden digitalen Plattformtechnologie für Services und Zahlungsdienste täglich Menschen in 46 Ländern weltweit bei ihrer Arbeit. Edenred vernetzt so 50 Millionen Arbeitnehmer seiner 850.000 Kundenunternehmen mit zwei Millionen kooperierenden Handelspartnern.

Edenred bietet zweckorientierte Bezahllösungen für Food (Essensgutscheine), Mobilität (z. B. Multi-Energie-, Wartungs-, Maut-, Park- und Pendlerlösungen), Incentives (Geschenkgutscheine, Mitarbeiter-Incentive-Portale) und Payment Solutions für Unternehmen (virtuelle Bezahlräume). Diese Angebote erhöhen – gemäß Edenreds Purpose „Enrich Connections. For good." – den Wohlfühlfaktor der Mitarbeiter im Unternehmen wie auch ihre Kaufkraft. Sie steigern die Attraktivität und Effizienz der Unternehmen und beleben den Mitarbeitermarkt wie die lokale Wirtschaft. Sie fördern auch den Zugang zu gesünderen Lebensmitteln, umweltfreundlicheren Produkten und besserer Mobilität.

Alle 10.000 Mitarbeiter von Edenred haben sich zum Ziel gesetzt, die Arbeitswelt zu einem miteinander verflochtenen Ökosystem zu machen, das täglich sicherer, effizienter und anwenderfreundlicher wird.

Im Jahr 2020 erzielte die Gruppe mit ihrem weltumspannenden Technologiesystem ein Geschäftsvolumen von fast 30 Milliarden Euro, das hauptsächlich mittels mobiler Anwendungen, Online-Plattformen und Gutscheinkarten erreicht wurde.

Edenred ist an der Pariser Börse Euronext notiert und geht in die Berechnung der folgenden Indizes ein: CAC Next 20, CAC Large 60, Euronext 100, FTSE4Good und MSCI Europe.

Weitere Informationen: www.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