Внимание, капан!

Измами с горивни карти и как да ги предотвратим

Бъди разумен:
Защити своята карта

Съдържание

01

Измами с горивни карти в Европа

Анализи и стратегии за гарантиране сигурността на карти и транзакции

Картите за гориво и безконтактните устройства за плащане на пътни такси се превърнаха във важни оперативни инструменти за търговските пътнотранспортни оператори в цяла Европа, като се има предвид броят на автомагистралите, мостовете и тунелите с такса в региона и това, че шофьорите разчитат на бензиностанциите, за да им помогнат да достигнат до европейски дестинации безопасно и своевременно.

Като се има предвид удобството, което картите за гориво и безконтактните устройства за плащане на пътни такси осигуряват на шофьорите, видимостта и контролът, които те предоставят на работодателите, и глобалната тенденция към безкасови методи за разплащане, не е учудващо, че употребата им се увеличава. Allied Market Research изчислява, че стойността на световния пазар на горивни карти, регистрирана при 672 милиарда долара през 2019, ще се удвои до 1,2 трилиона долара до 2027.

Недостатъкът на популярността на тези карти, обаче, е нарастващият риск от измами. Всъщност, инцидентите с измами значително се увеличиха през годините, тъй като престъпниците използват все по-сложни техники, за да проникнат в сигурността на картите и устройствата за разплащане.

Проблемът стана по-остър по време на пандемията от КОВИД-19, тъй като повече транзакции се извършват онлайн. Случаите на измами са били повече през 2020, отколкото през 2019, като голяма част от увеличението се наблюдава при измами, свързани с пътни такси, тунели и мостове.

Като се има предвид нивото на потребление и цената на горивото, както и мащабът на много съвременни автопаркове, горивото е един от най-високите разходи, които всеки транспортен оператор трябва да понесе и може да представлява до 30% от текущите разходи на автопарка. По този начин всяка манипулация, злоупотреба или кражба на горивни карти може да има сериозно въздействие върху рентабилността и потенциала за загуби на десетки хиляди евро за дни.

01

Примери на измама от последните години:

- През 2015 разследващите от Федералната служба за криминална полиция на Германия задържаха престъпна група фалшификатори на карти за гориво, които, според съобщенията, нанесоха щети на стойност 3,5 млн. евро в цяла Европа чрез скимиране на карти.
- В случай от 2017 австрийските власти, заедно с баварската и италианската полиция, разследват осем заподозрени, за които се твърди, че са откраднали 288 карти за пътни такси и гориво от паркирани камиони и са причинили щети в размер на 1 милион евро.
- През 2020 в Германия шофьор на камион с две манипулирани карти за гориво открадна дизел на стойност приблизително 100 000 евро.

На този фон не е учудващо, че защитата и сигурността от измами са важен фактор за клиентите, когато става въпрос за избор на доставчик на услуги за горивни карти.[1]

Целта на тази бяла книга е да даде на мениджърите на автопаркове и професионалните шофьори представа за проблема с измамите с карти за гориво, за да се повиши осведомеността за рисковете за сигурността и превантивните мерки. Екипът на UTA по измамите и сигурността на картите идентифицира начина на действие и „горещите точки“ на регионалните измами в Европа, чрез които се извършват различни видове измами с карти.

Случаите на измама нарастват.

1. Източник: Datamonitor

02 Видове измами с горивни карти

Измама със скимиране и копиране на карти

Има много видове измами, с които операторите на пътния транспорт и на автопаркове трябва да са наясно. Досега, най-често срещаният тип е измамата със скимиране и копиране на карти, които заедно представляват по-голямата част от всички измами през последните три години.[2]

Измами със скимиране и копиране на карти са случаите, при които данните за картата се откраднат по време на транзакция на мястото на продажба от касата или чрез четеца на карти. Понякога тя се извършва заедно с картодържателя в замяна на пари, често в зоните за почивка на шофьорите. UTA изчислява, че на замесените в измамите притежатели на карти се плаща приблизително 1000 евро на карта.

Откраднатите данни се използват за създаване на копирана карта, често направена така, че да имитира истинска (може би изтекла) карта за гориво, за да се избегне подозрение в случай на спиране и претърсване от полицията.

Все по-често престъпниците използват технологии като Bluetooth и WiFi за предаване на данни от карти от скимиращи устройства, които са били поставени в четци на карти. Като алтернатива, престъпниците понякога поставят улавящи устройства в четци на карти, които предотвратяват връщането на карти на картодържателя. Те се използват заедно с малка камера за заснемане на ПИН кода при въвеждането му.
След като картодържателят се върне в автомобила си, престъпникът премахва устройството и картата. Веднъж копирани, с картите обикновено се злоупотребява в станции без персонал или извън терминали за плащане в обслужвани станции на място, различно от мястото, където са били скимирани, често през нощта или през уикенда.

По-традиционните форми на измама с копиране на карти включват „сърфиране през рамото“ – при което престъпниците наблюдават как потребителят въвежда своя ПИН; или проникване в паркирано превозно средство, обикновено в зона за почивка или специално място за паркиране на камиони, за да копират данните на картата. Измамниците знаят, че шофьорите на камиони често оставят лепенки в кабините си с данни за картите и ПИН. След като намерят и копират информацията, те често излизат от превозното средство без следа, оставяйки шофьорите в неведение, че картите им са компрометирани.

Чип & ПИН картите предлагат известна защита срещу скимиране, но не са недосегаеми поради настоящото връщане към магнитна лента, когато чипът е повреден или нечетлив. Измамниците просто ще повредят чипа, като го надраскат и го покрият с фалшив стикер, така че да не може да се използва, или като просто разбият чипа с чук.

Скимирането и копирането на карти са най-честите типове измама.

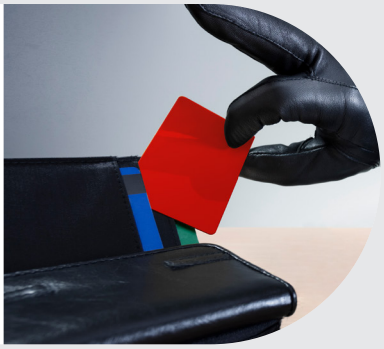
2 Според AI Corp, 97% от случаите в Италия са свързани със скимиране през 2019

02

В допълнение към измамите със скимиране и копиране на карти, другите видове измами с карти включват:

Измама с изгубена и откраднатa карта

Когато престъпниците крадат карти и, където е възможно, ПИН кодове. Дори и без ПИН, откраднатите карти могат да бъдат използвани с измама в мрежи, които не изискват ПИН, като например онлайн покупки в мрежата. Повечето измами се отнасят до покупки с карти, преди те да бъдат открити или докладвани като изгубени или откраднати, или покупки с карти поради забавяне на включването в черния списък или ограничени квоти в черния списък.



Заговор в обект

В тези случаи шофьорите са в заговор с персонала на обекта, за да извършват транзакции за гориво, когато не е извършено презареждане, или да таксуват повече за горивото. Стойността често се обменя за пари в брой или стоки като цигари. Това понякога се нарича „дизелизация“. Информацията за обекти, склонни към тайни споразумения, често се предава между шофьорите.

Злоупотреба с оригинална карта от притежателя на картата (измама от шофьор)

Когато картата се използва за цели, различни от тези, за които е оторизирана. Например, закупуване на гориво за друго превозно средство или шофьор в замяна на пари в брой; закупуване на гориво с валидна карта, но изсмукване на горивото от резервоара; използване на „мек резервоар“, скрит вътре в превозното средство; повреда на чип или магнитна лента, за да се отменят контролите за покупка или да се оправдае плащането на гориво с пари в брой, за да се скрие покупката на неразрешени стоки; или шофьори, използващи данни за карти от предишни компании и т.н. Измамите от шофьори са особено трудни за идентифициране, тъй като са склонни да следват „нормалното“ за шофьора поведение при покупка.

Вътрешна измама

Тук служителите или контрагентите действат самостоятелно или в тайно споразумение с външни страни (доброволно или поради принуда или подкуп) за кражба на данни, информация или материали от чувствителен търговски характер или които биха могли да бъдат използвани за компрометиране на операциите или сигурността на компанията.

02

Измама с неполучаване/прихващане на поща

Това включва прихващане на карти и/или ПИН кодове на адрес на клиента, в център за сортиране на поща или в рамките на пощенската система за разпространение. Компрометираните карти се копират, изпращат се отново и се доставят на клиента. Клиентите, които са най-застрашени, са предприятия с комунални пощенски кутии или тези, които нямат пренасочване на поща, когато променят адреса си. По подобен начин, известно е, че карти и ПИН кодове се прихващат в центровете за сортиране на поща на летищата и другаде.

Измами със самоличност и приложение

Престъпниците понякога се представят за или поемат истински бизнес, за да открият сметка, използвайки фалшиви или откраднати документи. Ако фалшивото заявление е успешно, измамниците получават карти и достъп до други услуги, издава им се фактура няколко дни преди падежа на плащането, което им дава достатъчно време да извършат измама. Неплащането на фактура често е причината за разкриването на измамата.

Измама с липса на карта

Това включва кражба на данни за карта, използвана за извършване на онлайн покупка, оставяйки истинския картодържател в неведение, докато не провери извлечението си. Престъпниците получават номерата на карти за гориво с помощта на специален софтуер, който генерира валидни номера на карти, или чрез скимиране и пробиви на данни и след това продават картите на шофьори, които ги използват в тол мрежи. Престъпниците (обикновено бивш служител) влизат в онлайн портали, за да поръчат фериботни билети, евровинетки и пътни такси, като използват данните на картата на предишната си компания за превозните средства на друга (обикновено за техния настоящ работодател или евентуално собственик-шофьор, с когото са в тайно споразумение).

Клониране на превозно средство

В този сценарий регистрационният номер на истинско превозно средство се копира и използва за друго превозно средство от същата марка и модел с цел избягване на плащания за гориво, пътни такси и паркинг, такси за задръствания и др.

02 Профилът на измамник

Следните характеристики са типични за измамниците[3]:

69% са на възраст между **36-55** години

79% са **мъже** (но процентът на жените нараства)

62% вероятно са в **заговор** с други

65% са служители, извършващи измамни действия **срещу техния собствен работодател**

35% са членове на **висше ръководство** (включително членове на съвети))

38% са работили в компанията си най-малко **шест години**, преди да извършат измама

Измамите с голям мащаб обикновено включват висши членове на ръководството, които отменят контрола на ниво процес чрез високото си ниво на власт.

В допълнение, измамниците обикновено:

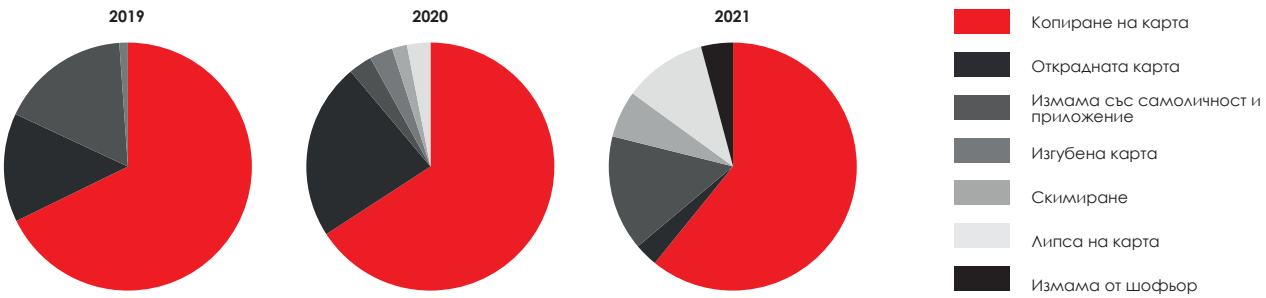
- Не вземат отпуски
- Са потайни относно бизнес процесите
- Са устойчиви на надзор
- Имат лоши междуличностни умения
- Имат добри технически способности
- Работят до късно
- Са предразположени към злоупотреба със субстанции/алкохол
- Са предразположени към конфликти във взаимоотношенията

3 Източник: KPMG Global Profiles of the Fraudster, 2016

02

Примери на развитието на измамите в Европа 2019-2021

Принос на типа измама към общите загуби на година



Тъй като заплахите от измама се променят постоянно, редовните оценки на риска и непрекъснатото развитие на методите за превенция и откриване са жизненоважни за поддържане на високи нива на сигурност.

Измамата с карти се развива:

- От отделни престъпници към организирани и международни престъпни групи
- От скимиране на една карта до атаки, свързани с достъп до данни
- От престъпници, работещи през целия жизнен цикъл на измамите, до измамници, специализирани в част от тази верига на стойността и продаващи тази стойност на следващото ниво

Измамниците се усъвършенстват все повече чрез:

- Спуфинг на устройства
- Манипулиране на локации
- Заплахи и интернет измами
- Приемане на фалшива дигитална самоличност
- Маскиране като клиенти
- Предлагане на измами като услуга (FaaS) често чрез „тъмната мрежа“ – извършвано или от глобални престъпни синдикати, или от еднолични измамници

03

Регионалност на измамите с карти

Горещи точки и регионални тенденции в Европа

В днешната дигитална ера техниките за измама стават все по-сложни с всеки изминал ден. В миналото, престъпниците обикновено копираха една карта за гориво, но днес те често произвеждат множество версии и ги разпространяват едновременно на познати конспиратори в различни държави за максимална финансова печалба. За да се извърши такова постижение, престъпниците трябва да бъдат организирани. И наистина, много от тях са – често част от по-големи престъпни групи, действащи в цяла държава и участващи в търговия с наркотици, трафик на хора, търговия с оръжие или още по-лошо.

Организираните престъпни групи са разпространени в цяла Европа4 и много от тях са съсредоточили географски усилията си за измами. Анализът показва, че една престъпна група се съсредоточава върху сервизните станции по автомагистралите на главните кръстовища изток-запад или север-юг във Франция, докато друга се концентрира върху южната граница на Холандия, където граничи с Белгия и Германия. Последните открития показват значително увеличени престъпни дейности по маршрута от Бордо до Ирун в Испания, по източното крайбрежие на Италия и по маршрутите, водещи от Италия до Словения. Освен това, френската граница с Германия и Швейцария показа повишение на случаите на измами с карти през последните месеци.

Други престъпни групи са насочени към шофьори въз основа на тяхната страна на произход – страни, в които може да имат съконспиратори, които помагат за извършването на измамата. Например, има съмнения, че престъпни групи във Франция и Холандия може да имат връзки с Източна Европа и може да са насочени към шофьори от този регион. Сигурно е, че повечето евровинетки, закупени чрез измама онлайн, са за превозни средства на компании, базирани в Източна Европа.

Като цяло, измамата отразява успеха на транспортните компании, базирани в Източна Европа, преместващи стоки на запад и на юг през Италия и Франция през Испания и на север до Скандинавия и обратно.

Горещи точки на измами
2019 - 2021

По-специално Франция се превърна в гореща точка за измами поради статута си на транспортен център и поради преобладаващия брой бензиностанции без персонал. По-голямата част от скимирането се извършва в станции без персонал на север и изток от Париж и в основните транспортни центрове около Лион и Гренобъл. По на юг, Перпинян видя скок в престъпността през първото тримесечие на 2021.

Бензиностанциите и зоните за почивка по френско-испанската граница и в граничния район Венло на Холандия са основните места за влизане с взлом в превозни средства и злоупотреба с копирани карти.

Мониторингът на честотата на измамите и географското разпределение е полезен за предотвратяване на измами и за бързо реагиране в случай на такива.

4 Източник Европол: Една масова атака с копиране в Холандия, използваща вратички в скоростта, отне 800 000 долара в рамките на седмици. В Италия атака в рамките на границите на скоростта на място отне 3,2 милиона долара за по-малко от два месеца. През 2018 Европол разби испанска престъпна група, използваща фалшиви карти за гориво в рамките на испански и френски тол мрежи: извършени са 24 ареста, 600 регистрации на превозни средства са компрометирани, 11 фабрики за карти са демонтирани, 15 000 фалшиви карти са иззети, като е идентифицирана и загуба от 500 000 евро.

04 Стратегии за предотвратяване на измами с горивни карти

Какво може да се направи, за да се намали рискът от измами с карти и да се осуетят непрекъснато развиващите се усилия на престъпниците? Като начало, издателите на карти, мениджърите на автопаркове, партньорите и потребителите на карти трябва да работят заедно, за да постигнат най-високи нива на сигурност.

4.1 Мерки за доставчиците на горивни карти

Тъй като измамите с карти за гориво се превърнаха в заплаха в цяла Европа, водена от международни престъпни групи, разкриването и наказателното преследване изискват сътрудничеството на международните институции и власти. Два основни органа в тази област са Бюрото за разследване на измами с карти в горивната индустрия (FICFIB), група издатели на карти, търговци на дребно на горива и независими оператори на бензиностанции, които споделят информация за тенденциите, уязвимите места и развиващите се заплахи; и Европол, който споделя информация за трансгранични инциденти с местните полицейски сили, за да подпомогне при инциденти с клиенти и разследвания. Тясното сътрудничество с институциите дава на доставчиците на карти необходимото международно влияние за успешни действия в случай на инцидент.

В допълнение към сътрудничеството с власти и институции, за доставчиците на карти е от решаващо значение да създават, непрекъснато да наблюдават – и ако е необходимо – да оптимизират собствените си продукти, услуги и процеси. Това започва със създаването на продукти и услуги като известия за транзакции и включва редовното квалифициране на обслужването на клиентите и ИТ процесите, за да се гарантира, че може да се противодейства на престъпната дейност в реално време възможно най-бързо.

И накрая, комуникацията е решаващ компонент на сигурността на картите. Комуникационните процеси с власти, партньори и клиенти трябва да бъдат бързи и фокусирани.
В случай на измама бързата комуникация с всеки засегнат е от решаващо значение. Освен това е важно да се повиши осведомеността сред клиентите и партньорите относно опасностите от измама с горивни карти и да им се предложи подкрепа за нейното предотвратяване.

04

4.2 Подходът на UTA за предотвратяване на измами с карти

Като доставчик на услуги за мобилност, горивните и сервизните карти са крайъгълен камък за портфолиото от продукти и услуги на UTA. Следователно, сигурността на картите и транзакциите е приоритет.

В центъра на усилията на UTA срещу измамите е специалният екип за измама и сигурност на карти, който покрива отговорности като:

- Известията за транзакции в реално време позволяват на клиентите да се намесят незабавно
- Предупреждаване на клиентите по телефона, ако бъдат открити подозрителни събития
- Разработване и прилагане на стратегии и процеси за ефективно откриване, предотвратяване и смекчаване на последствията от измамите
- Препоръчване на техники за ограничаване на риска от измама
- Сътрудничество с адвокати, служители на закона, FICFIB и други за разработване и изпълнение на планове за разрешаване на случаи на измами
- Разработване и наблюдаване на отчети и информация, полезни при залавянето на измамници
- Провеждане на интервюта с жертви и заподозрени с цел получаване на информация относно естеството на атаката и определяне на тяхното потенциално участие

"Чрез нашите продукти, услуги и процеси ние сме ангажирани да защитаваме нашите клиенти срещу настоящи и нововъзникващи форми на измами."

Карстен Бетерман,
Изпълнителен директор на UTA

Сигурността на картите и транзакциите са ключови фактори за успех в сектора на услугите за мобилност.

04

Използване на индустриално разузнаване

Една от причините за високия процент на откриване на измами на UTA е задълбоченият експертен опит по темата, натрупан през годините на сътрудничество с водещи организации за сигурност, браншови органи и експерти от трети страни.

Там, където UTA нямат вътрешен опит, те си партнират със специалисти – например в области като кибер криминалистика, възникващи заплахи за разплащателни карти и банкови продукти, търсене в мрежата или задълбочени разследвания на престъпления. Като пример, за базирано на алгоритъм автоматизирано и оптимизирано откриване на измами UTA си сътрудничи с The ai Corporation Ltd, специалист за управлявани от изкуствен интелект системи за сигурност на плащанията и мониторинг на транзакциите. Освен това UTA е член на FICFIB, координира се с Европол и е активен член на браншовите органи, които определят общи стандарти за сигурен обмен на данни между мрежите за приемане и издателите на карти.

Освен това UTA работи с оператори на бензиностанции в 40 европейски страни, за да гарантира, че имат сигурност в зоните на обществен достъп, като CCTV или IP камери, защита срещу инсталиране на скимиращи устройства и възможности за оторизиране на онлайн транзакции.

Като част от глобалната група Edenred, UTA се възползва от експертни познания в области като съответствие, поверителност на данните и ИТ сигурност. Дългогодишният форум за измами на Edenred обхваща всички направления на бизнеса им в повече от 50 държави, като споделя поглед отвътре и най-добри практики по теми, вариращи от видове измами до съдебни спорове.

Изкуственият интелект и машинното обучение са незаменими инструменти днес за ефективно предотвратяване на измами с карти за гориво и бързо откриване на случаи на измами. В нашето сътрудничество с UTA, ние комбинираме най-модерни технически системи (aiAutoPilotML) и ноу-хау на нашите експерти по карти за гориво с изчерпателния опит, който UTA предлага в областта на предотвратяването и откриването на измами с карти за гориво. Чрез този пакет от технологии, опит и експертни познания, ние постигаме много високо въздействие и успех в предотвратяването и борбата с измамите с карти за гориво."

Д-р Марк Голдспинк,

Изпълнителен директор на The ai Corporation Ltd

Комбиниране на вътрешен опит със специализирани партньори за постигане на оптимални резултати.

04

Заемане на проактивна, превантивна позиция

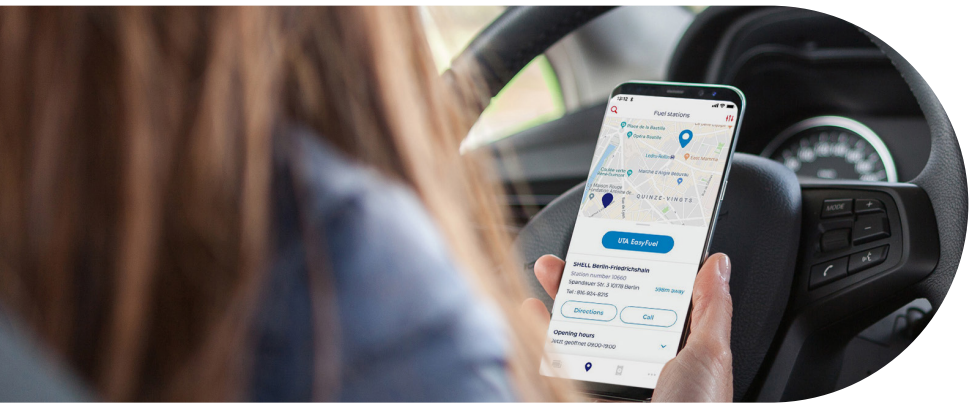
Наред с експертния си опит в областта, UTA прилагат превантивен подход, „сигурност по дизайн“, за да гарантират, че техните платформи и продукти са изградени от самото начало за максимална сигурност. Освен това компанията инвестира значително в научноизследователска и развойна дейност в области като анализ на данни, изкуствен интелект и машинно обучение, за да помогне на своя екип за измами и сигурност на карти да открие все по-разширяващия се диапазон от видове измами по-бързо от всякога.

Например, за да се борят с масовото фалшифициране на карти за гориво и пътни такси, UTA са внедрили проверки за географска достоверност, които проследяват времето и разстоянието между местата, за да се види дали е физически възможно транзакцията да бъде легитимна или не. Когато се установят проблеми, картите се блокират незабавно и клиентите се уведомяват.

Наличието на такава детайлна видимост на европейския пейзаж на измами позволява на екипа на UTA за измами и сигурност на карти да действа, за да сведе до минимум риска за клиентите, да привлече подкрепата на Европол и други органи по сигурността, ако е необходимо, и да споделя информация в FICFIB.

„В момента разработваме нашата нова цифрова карта за гориво. Това усъвършенствано решение съчетава опита на UTA в сигурността на транзакциите и предотвратяването на измами със задълбочените познания на нашата компания-майка Edenred в платежните услуги.“

Карстен Бетерман,
Изпълнителен директор на UTA



Цифрови карти за гориво - по-бързи, по-удобни и по-сигурни

Процедурите за безконтактно цифрово разплащане се увеличават – тенденция, ускорена от пандемията от КОВИД-19. Приложенията за цифрови карти за гориво на смартфон не само позволяват по-лесни покупки на гориво от колонката, но осигуряват по-бързи и по-ефективни процеси, от влизане и регистриране в системата до управление на собствени данни.

Друго предимство е допълнителната сигурност на транзакциите, който тези цифрови карти предоставят пред физическите карти за гориво.

04

Минимизиране на риска за клиентите

За да намали риска от картови измами за клиентите, UTA внедри набор от защитни функции и услуги. Те включват 24/7 блокиране на карти чрез онлайн портала на UTA, ПИН номера за всички карти, даващи възможност на клиентите да задават собствени лимити за разходи по картите, осигуряване на контрол върху това къде и кога могат да бъдат закупени продукти, както и прозрачно фактуриране и отчитане. Клиентите могат да ограничат сумата, която картите могат да купят, както и да ограничат дните от седмицата и часовете от деня, в които могат да бъдат използвани.

Услугата за известяване на транзакции на UTA предупреждава клиентите в реално време, когато се извършват транзакции с горивни карти UTA, което им позволява да се намесят, ако забележат нещо подозрително. Услугата може да бъде съобразена с изискванията на клиента – например филтрите могат да бъдат настроени да изпращат известия чрез текстово съобщение или имейл, за задаване на минимална стойност на транзакция за всяко предупреждение или за задаване на специфични за държавата ограничения за дата или час.

И накрая, UTA подкрепя клиенти, които стават жертва на измама, като се свързва с доставчика - например оператора на бензиностанцията – за да поиска да бъде запазено всяко видео или заснемане от CCTV за полицейски разследвания. Когато е уместно, екипът на UTA за измами и сигурност на карти се свързва с полицията, за да предостави информация, която може да бъде използвана като доказателство или за идентифициране на други потенциални жертви.

Успехи

В обобщение, UTA се стреми да предвиди, определи и неутрализира престъпната дейност, преди тя да засегне клиентите – позиция, в която се радва на висок процент на успех. Компанията идентифицира близо 90% от инцидентите, преди да бъдат забелязани от клиентите. Преди две години тази цифра беше 63%, което подчертава ефективността на усилията на компанията. Освен че забелязва повече инциденти с измами, UTA ги открива по-бързо, което позволява значително да намали средните загуби през последните години.

04

4.3 Най-добри практики за потребители на горивни карти

При всички усилия на издателите на карти да защитят клиентите, клиентите също трябва да се защитят сами, като гарантират, че картите им се пазят в безопасност и като смекчават риска от злоупотреба.

Ето някои най-добри практики, които клиентите да следват:

За шофьори:

Безопасност на PIN
Потребителите на карти трябва да запомнят своя ПИН номер и никога да не го записват там, където може да бъде открит заедно с тяхната карта. ПИН номерата никога не трябва да се маскират като дата на раждане или телефонен номер на мобилно устройство, нито трябва да се разкриват на други лица. Освен това потребителите трябва да скриват своя ПИН, когато го въвеждат в платежно устройство.

Безопасност на картата
Шофьорите никога не трябва да оставят картата си без надзор в кабината на превозното си средство или в помещенията на компанията. Това увеличава шансовете тя да бъде копирана без тяхно знание.

Бдителност
Потребителите на карти винаги трябва да проверяват помпата за признаци на намеса и да съобщават за всичко подозрително. Най-безопасно е да се използва помпа близо до станция и с ясна видимост на касата и/или CCTV. Когато плащат на закрито, притежателите на карти трябва да избягват да дават картата си на касата за поставяне в платежно устройство и да се опитат да направят това сами. Освен това те трябва да внимават за подозрителни превозни средства, паркирани наблизо.

За управители на автопаркове:

Контрол на картата
Работодателите имат възможността да задават лимити за стойността, изразходвана по техните карти и колко често могат да се използват ежедневно или месечно. Могат да се задават допълнителни контроли за това какви продукти и услуги могат да бъдат закупени и къде.

Проверка на транзакции
Работодателите трябва да проверяват своевременно фактурите и разписките, за да гарантират, че всички плащания са законни. В допълнение, отчетите за километри на литър (KPL) за превозни средства трябва да бъдат наблюдавани, за да се идентифицират случаи на свръхпотребление.

04

Образоване на шофьори
Работодателите трябва да образоват своите шофьори относно личната отговорност; че злоупотребата с карти е едновременно измама и престъпление, което може да доведе до загуба на работата им и/или наказателно преследване. Освен това работодателите трябва да внедрят писмени споразумения с шофьорите – документи, подписани от шофьорите, за да покажат, че са запознати и са разбрали последствията от всяко неправомерно поведение при шофиране на служебно превозно средство.

Подаване на сигнал за подозрително поведение или инциденти
Работодателите трябва незабавно да подадат полицейски доклад, ако техните шофьори са потърсени от служители на обект или други за извършване на измама или ако са станали свидетели на тайно споразумение. Освен това те трябва да докладват за загуба или кражба на карти или ситуации, при които ПИН номера са били компрометирани. Важно е да се докладва за инциденти в полицията в държавата, в която е извършено престъплението, както и в държавата на пребиваване. Това може да ускори трансграничното сътрудничество между силите и потенциално да доведе до по-бърз и по-успешен изход от случая.

Внедряване на „меки“ контроли
Много компании разчитат на сигнали, за да хванат измамници. Приблизително 43% от инцидентите се разкриват чрез податели на сигнали или други сигнали6. Въвеждането на система за подаване на сигнали може да има и икономически ползи: служителите и другите заинтересовани страни представляват първата линия на защита срещу скъпоструващо неправомерно поведение. Ранното откриване предоставя на организациите възможност да решат проблемите на ранен етап и да предотвратят финансови санкции и щети за репутацията.

Измамата често включва служители или висше ръководство, които са в състояние да отменят контролите чрез високото си ниво на власт. Превенцията изисква среда на работното място, която насърчава етичното поведение, възпира неправомерните действия и насърчава служителите да съобщават на правилното лице за всяко известно или предполагаемо неправомерно действие. Евентуалните измамници може да не са в състояние да извършат определени схеми за измами, ако служителите откажат да им помогнат и съдействат в извършването на престъпление. Въпреки че „меките“ контроли за насърчаване на подходящо поведение на работното място са по-трудни за прилагане и оценяване в сравнение с традиционните „твърди“ контроли, те са най-добрата защита срещу измами, включващи висшето ръководство.

5 Източник: KPMG

05

Как да се докладва измама с горивни карти

Отговори на често задавани въпроси

В случай на предполагаема или потвърдена измама, моля, имайте предвид следното:

На кого да се обадя в случай на инцидент?

Моля, свържете се незабавно с UTA, ако транзакция чрез UTA карта ви изглежда подозрителна или ако не сте изпълнили транзакцията. Можете да блокирате картата си, като се обадите на 00 800 88 22 62 26 или чрез клиентския център на UTA. След това подайте сигнал в местната полиция.

Защо трябва да подавам сигнал в полицията?

Измамата и злоупотребата с карти за неоторизирани транзакции са криминални престъпления. Имайте предвид, че може да не сте единствената жертва и че извършителят може да е свързан с други тежки престъпления. За да преследвате по съдебен път тези измамници, трябва да докладвате всеки случай на измама или злоупотреба в полицията. Полицията има много по-големи правомощия да разследва и осигурява доказателства от вас като физическо лице.

Кога трябва да подам сигнал?

Трябва да се свържете с полицията веднага след разкриване на измамата, тъй като престъплението може все още да продължава. Доказателствата, които могат да бъдат полезни за полицията, като видеозаписи, обикновено се съхраняват само за ограничен период от време. Срокът на задържане може да варира в зависимост от законовите изисквания на държавата, в която е извършено престъплението.

Къде трябва да докладвам инцидента?

Ако работите на международно равнище, трябва да помислите да докладвате за инцидента в полицията в страната, където се е случил инцидентът, и във вашата страна. Това е така, защото в случай на трансгранична измама може да се наложи полицията да си сътрудничи за разследвания и наказателно преследване.

Каква информация трябва да разкрия?

Всяко разследване е различно, но работодателите трябва да са готови да предоставят информация, поискана от полицията, като:

- Фирмени детайли, включително адрес и ДДС номер
- Описание на инцидента, включително номер на картата/BIN, място, дата и час, размер на кражбата
- Подробности за това къде обикновено се съхраняват картата и ПИН кодът
- Дали все още имате картата
- Дали картата е била блокирана и ако е така, кога
- Къде са били вашите шофьори точно преди инцидента – например: презареждане с гориво, паркиране или почивка
- Всяка друга свързана информация

06

Заключение

Осведоменост, бдителност, наблюдение, правилните технологии и бърза реакция в случай на инциденти: Всички те са ключови фактори за минимизиране на рисковете от измама с карти за гориво.

Измамите с карти за гориво се увеличават и причиняват значителни финансови загуби на компаниите всяка година.

Поддържането на актуални познания за най-новите тактики за измами и регионалните заплахи, стриктното проверяване на транзакции и разплащания и гарантирането на обучени и бдителни шофьори могат да се окажат изключително важни за защитата на автопарковете от измамници.

В допълнение, прилагането на правилните технически инструменти и мерки за сигурност може да доведе до по-ранно откриване на измамата и по-бърз и по-ефективен отговор.

В крайна сметка, най-добрата защита срещу измами с карти за гориво се основава на непрекъснато, ефективно сътрудничество между операторите на автопаркове и доставчиците на карти за гориво.

В UTA сигурността и защитата на клиентите са на първо място. Компанията ще продължи да инвестира и да прави иновации в стремежа си да овладее всички форми на измами и да сведе до минимум рисковете за клиентите.

Научете повече

За допълнителна информация относно измамите с карти за гориво и карти за пътни такси или за да научите повече за политиките на UTA, най-добрите практики за сигурност или технологични решения, моля, свържете се с:

Дейвид Джоунс
Ръководител по сигурността на плащанията, UTA
Директор Корпоративно развитие,
Решения за автопаркове & мобилност, Edenred

david.jones@edenred.com

За UTA

UNION TANK Eckstein GmbH & Co. KG (UTA) е водещ доставчик на горивни и сервизни карти в Европа. Търговските клиенти могат да използват картовата система на UTA за зареждане – независимо от марката и без пари в брой – в повече от 68 000 приемателни пункта в 40 европейски страни. UTA картата може да се използва и за фактуриране на пътни такси, ремонтни дейности и услуги, свързани с повреда и теглене.

Освен това възстановяването на ДДС и данък върху горивото може да бъде поискано чрез партньор на доставчик на услуги UTA.

UTA беше избрана за „Най-добър доставчик на услуги за карти за гориво за МСП 2021“ в проучване, проведено от немското списание Wirtschaftswoche и базирания в Кьолн институт за пазарни проучвания ServiceValue. UTA е основана през 1963 г. от Хайнрих Екщайн и днес е собственост на Edenred SE.

За повече информация: uta.com

За Edenred

Edenred е водеща дигитална платформа за услуги и плащания и ежедневен спътник за хората на работа, свързваща над 50 милиона потребители и 2 милиона партньори търговци в 46 страни чрез повече от 850 000 корпоративни клиенти. Edenred предлага решения за плащания със специфична цел за храна (като обезщетения за хранене), мобилност (като мултиенергийни, поддръжка, тол такси, паркиране и пътуване до работното място), стимули (като карти за подаръци, платформи за ангажиране на служители) и корпоративни плащания (като като виртуални карти).

В съответствие с целта на групата „Обогатете връзките. Завинаги." тези решения подобряват благосъстоянието и покупателната способност на потребителите. Те подобряват привлекателността и ефективността на компаниите и оживяват пазара на труда и местната икономика.

Те също така насърчават достъпа до по-здравословна храна, по-екологични продукти и по-гъвкава мобилност.

10 000 служители на Edenred се ангажират да превърнат света на работа в свързана екосистема, която е по-безопасна, по-ефективна и по-отговорна всеки ден.

През 2020, благодарение на своите глобални технологични активи, Групата управлява близо 30 милиарда евро в бизнес обем, основно осъществяван чрез мобилни приложения, онлайн платформи и карти.

Edenred е листван на фондовата борса Euronext Париж и е включен в следните индекси: CAC Next 20, CAC Large 60, Euronext 100, FTSE4Good и MSCI Europe.

За повече информация: edenred.com

УТА България Сървисис ЕООД
Бул. Проф. Яким Якимов 3, 8010 Бургас, България
Т/ +359 56 59 84 48 - contact.bulgaria@uta.com – uta.com/bg

We connect, You win