

La naturaleza cambiante del fraude con tarjetas de combustible (Parte 1)

Carsten Bettermann, director general de UTA, y Mark Goldspink, director general de The ai Corporation, analizan el creciente riesgo de fraude en el ecosistema de las tarjetas de combustible en Europa.

Las tarjetas de combustible y los dispositivos de liquidación de peajes sin contacto se han convertido en herramientas operativas fundamentales para los operadores de transporte comercial por carretera en toda Europa. Dado el número de autopistas, puentes y túneles de peaje en la región, y la dependencia de los conductores de las estaciones de servicio para ayudarles a llegar a sus destinos en toda Europa de forma segura y puntual, la tecnología se utiliza ahora para garantizar que las cadenas de suministro permanezcan abiertas y eficientes.

Dada la comodidad que las tarjetas de combustible y los dispositivos de liquidación de peajes sin contacto ofrecen a los conductores, la visibilidad y el control que proporcionan a los empresarios, y la migración mundial hacia métodos de liquidación sin efectivo, no es de extrañar que su uso esté en aumento. En muchos casos, ambas tecnologías se han convertido en herramientas de gestión de gastos fundamentales para muchos en el sector del transporte por carretera. Allied Market Research estima que el valor del mercado mundial de tarjetas de combustible, registrado en 672.000 millones de dólares en 2019, casi se duplicará hasta alcanzar los 1,2 billones de dólares en 2027.

Sin embargo, como todos los canales de pago, especialmente los que están en crecimiento, como las tarjetas de combustible, existe un riesgo creciente de fraude. De hecho, los incidentes de fraude han aumentado significativamente a lo largo de los años, ya que los delincuentes emplean técnicas cada vez más sofisticadas para infiltrarse en la seguridad de las tarjetas y los dispositivos de liquidación. El fraude se ha vuelto más común durante la pandemia de COVID-19, ya que se realizan más transacciones en línea y el valor de las transacciones individuales aumenta. Los casos de fraude fueron más altos en 2020 que en 2019, y gran parte del aumento se produjo en el fraude relacionado con peajes, túneles y puentes.

Dado que la compra de combustible representa hasta el 30% de los costes de funcionamiento de una flota, cualquier manipulación, mal uso o robo de las tarjetas de combustible podría tener un grave impacto en la rentabilidad y el potencial de pérdidas de decenas de miles de euros en días.

El fraude con tarjetas evoluciona y se extiende por toda Europa

De los delincuentes individuales a los grupos delictivos organizados e internacionales; del robo de una sola tarjeta a los ataques de violación de datos; y de los delincuentes que trabajan en todo el ciclo de vida del fraude a los defraudadores que se especializan en una parte de esa cadena de valor y venden ese valor al siguiente nivel.

Al mismo tiempo, los defraudadores son cada vez más sofisticados:

- Falsificación de dispositivos
- Manipulación de la ubicación
- Amenazas y bots
- Fraude empresarial
- Asumir identidades digitales fraudulentas
- Hacerse pasar por clientes

Oferta de fraude como servicio (FaaS), a menudo a través de la web oscura, llevada a cabo por sindicatos criminales globales o por estafadores solitarios

En la era digital actual, las técnicas de fraude son cada vez más sofisticadas. En el pasado, los delincuentes solían copiar una sola tarjeta de combustible, pero hoy en día suelen producir múltiples versiones y distribuir las simultáneamente a compañeros de conspiración en diferentes países para obtener el máximo beneficio económico. Para llevar a cabo esta hazaña, los delincuentes deben estar organizados. Y, de hecho, muchos lo están: a menudo forman parte de bandas más grandes que se dedican al tráfico de drogas, de personas, de armas o de cosas peores.

Las bandas organizadas abundan en toda Europa(1), y muchas de ellas han adoptado un enfoque geográfico para sus esfuerzos de fraude. Los análisis indican que una banda se centra en las estaciones de servicio de las autopistas en los principales cruces este-oeste o norte-sur de Francia, mientras que otra se concentra en la frontera sur de los Países Bajos, donde colinda con Bélgica y Alemania.

Los últimos descubrimientos indican un aumento significativo de las actividades delictivas a lo largo de la ruta de Burdeos a Irún en España, en la costa oriental italiana y en las rutas que llevan de Italia a Eslovenia. Asimismo, en la frontera francesa con Alemania y Suiza se ha producido un aumento de los incidentes de fraude con tarjetas en los últimos meses.

Otras bandas tienen como objetivo a los conductores en función de su país de origen, países en los que pueden tener cómplices que les ayuden a perpetrar el fraude. Por ejemplo, se sospecha que las bandas de Francia y los Países Bajos pueden tener vínculos con Europa del Este y pueden dirigirse a conductores de esa región. Lo cierto es que la mayoría de las euroviñetas compradas fraudulentamente en línea son para vehículos pertenecientes a empresas con sede en Europa del Este.

En general, el fraude está reflejando el éxito de las empresas de transporte con sede en Europa del Este que mueven las mercancías hacia el oeste y el sur a través de Italia y Francia hasta España y hacia el norte hasta Escandinavia y de vuelta. Francia se ha convertido en un punto caliente de fraude debido a su condición de centro de transporte y a la prevalencia de estaciones de servicio sin personal.

La mayor parte de los robos se producen en las estaciones no vigiladas del norte y el este de París y en los principales centros de transporte de Lyon y Grenoble. Más al sur, en Perpiñán, se produjo un repunte de los delitos en el primer trimestre de 2021. Las estaciones de servicio y las áreas de descanso a lo largo de la frontera franco-española y en la zona fronteriza de Venlo, en los Países Bajos, son los principales lugares donde se producen robos de vehículos y el uso indebido de tarjetas copiadas.

No cabe duda de que el seguimiento de los índices de fraude y la distribución geográfica puede ser muy útil para prevenir el fraude y poder reaccionar rápidamente si se produce. Sin embargo, es imperativo que sigamos centrándonos en mejorar la tecnología y las medidas preventivas dentro del ecosistema de las tarjetas de flota. Para hacerlo con eficacia, necesitamos saber dónde y cómo aprenden los individuos las técnicas para cometer fraudes y la racionalización de su actividad delictiva. También tenemos que evitar que se creen lagunas en los procesos, en los que los individuos puedan verse tentados a cometer un fraude, adoptando un enfoque de lección aprendida constante, por lo que la comunicación y la colaboración como agentes de prevención del fraude son fundamentales. Quedarse quieto no es una opción.

(1) Fuente Europol: Un único ataque de copia masiva en los Países Bajos que aprovechaba las lagunas de velocidad se llevó 800.000 dólares en pocas semanas. En Italia, un ataque dentro de los límites de velocidad in situ se llevó 3,2 millones de dólares en menos de dos meses. En 2018, Europol desarticuló un grupo delictivo español que utilizaba tarjetas de combustible falsificadas dentro de las redes de peaje españolas y francesas: se realizaron 24 detenciones, se comprometieron 600 registros de vehículos, se desmantelaron 11 fábricas de tarjetas, se incautaron 15.000 tarjetas falsificadas y se identificó una pérdida de 500.000 euros.

Se publicará la segunda parte de este artículo.

Escrito por **Carsten Bettermann**, director general de UNION TANK Eckstein GmbH & Co. KG (UTA) y **Mark Goldspink**, director general de The ai Corporation (ai). Ambas empresas trabajan juntas para prevenir y detectar el fraude. Puede encontrar más información sobre el complejo campo del fraude en las tarjetas de combustible y las medidas de prevención que deben tomarse aquí.