Fraude en Telecomunicaciones

Definición de fraude

- Según la RAE

m. Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.
m. Acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros.

- Según el Código Penal Español

El fraude es un acto ilegal realizado por una o varias de las personas que se encargan de vigilar el cumplimiento de contratos públicos o privados para obtener algún provecho.

Y si nos centramos en el Fraude en Telecomunicaciones en nuestro código penal
art 255
Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación utilizando energía eléctrica, gas, agua, **telecomunicaciones** u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1.º Valiéndose de mecanismos instalados para realizar la defraudación.
2.º Alterando maliciosamente las indicaciones o aparatos contadores.
3.º Empleando cualesquiera otros medios clandestinos.

Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses.

art 256
El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, y causando a éste un perjuicio económico, será castigado con la pena de multa de tres a doce meses.
Si la cuantía del perjuicio causado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses.

- Según una de las principales operadoras de nuestro país

El fraude en servicios de telecomunicación es el uso indebido e intencionado de redes, productos y servicios, que produce pérdidas económicas y/o de imagen a una operadora o a sus clientes y beneficios a quien las realiza.
El defraudador es toda persona o entidad que, al utilizar indebida e intencionadamente los productos, redes y servicios de una Operadora, produce pérdidas económicas y/o de imagen a la misma en beneficio propio.

Introducción

El sector de las Telecomunicaciones es uno de los que más sufren el efecto negativo de estos tipos de actos delictivos pese a que es también uno de los más avanzados tecnológicamente, pero el número de potenciales víctimas (más de 5.000 millones de personas utilizan un teléfono móvil) y la facilidad con la que se pueden contratar sus servicios vía telefónica o por internet, hacen que sea uno de los objetivos principales de los defraudadores.
Según las últimas encuestas las **pérdidas por fraude** de las empresas de Telecomunicaciones están en la horquilla **de 29.000-32.000 millones de dólares**
Además de las perdidas, el impacto del fraude en una operadora conlleva unos costes tanto directos como indirectos

- Costes directos
  - Pagos por interconexiones.
  - Pagos a terceras partes.
  - Costos administrativos (Ventas, Facturación, cobros)
  - Reclamaciones relacionadas a fraude.
  - La propia gestión del fraude.
- Costes indirectos
  - Planificación del mercado basado en niveles elevados de fraude.
  - Impactos negativos en los clientes y en la imagen de la compañía.
  - Inversiones de redes, sistemas, … basados en datos erróneos.

Todos conocemos el "iceberg" de internet donde solo se nos muestra una pequeña parte de lo que en realidad es; con el fraude nos ocurre lo mismo, tenemos lo visible (el fraude detectado, las pérdidas conocidas) y tenemos la parte no visible, mucho más grande por lo general (fraude no detectado, pérdidas desconocidas)

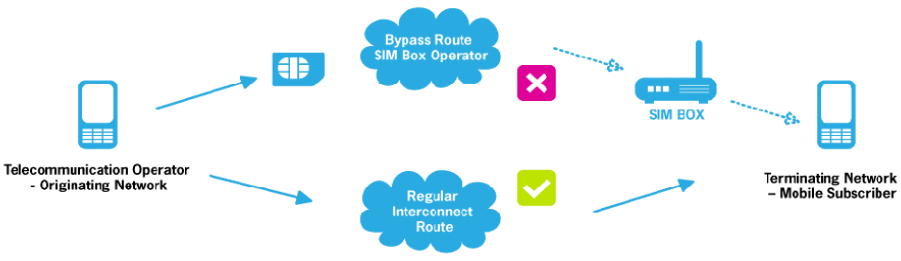
En este artículo, vamos a tratar de dar una visión, intentando no ser demasiado técnico en la explicación, de una pequeña muestra de los principales fraudes que se cometen contra las operadoras de telecomunicaciones y de un tema que afecta como mal endémico al sector de la seguridad y al rol de Director de Seguridad, que es el intrusismo, en este caso interno, (he querido utilizar este término de intrusismo aunque realmente se trata en muchos casos de luchas de ego y poder internas, de decisiones en muchos casos erróneas en la asignación de responsabilidades, etc.…) y las funciones del área de seguridad en este ámbito

Principales fraudes en una operadora de telecomunicaciones

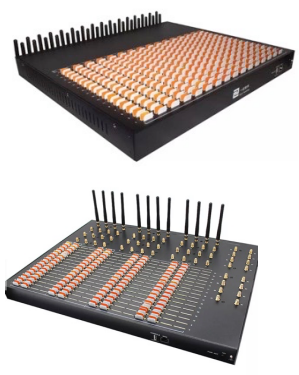
- **Fraude de suscripción** es la modalidad de fraude más común y que es además la puerta de entrada a la realización de otros tipos de fraude, donde el defraudador falsea y altera su información para solicitar el alta de líneas, paquetes de datos, servicios que ofrece la operadora como puede ser la televisión de pago, la compra de teléfonos de alta gama a plazos, etc....
Por lo general, **suele ir unido a una usurpación de identidad**, por lo que no solo se altera la información, sino que utiliza la identidad de una tercera persona para obtener estos productos o servicios sin intención de pagar.
Estos datos de terceras personas se pueden obtener por distintas fuentes y/o técnicas como el phishing, vishing, malware, ingeniería social, robo de información física (facturas o extractos bancarios en el buzón de casa), compra de datos en la dark web, etc…
Es por ello, que la función de prevención del fraude debe estar "pegada" a Seguridad de la Información y trabajar conjuntamente para evitarlo

-**Fraude en Roaming**, consiste en la adquisición de tarjetas SIM por medios fraudulentos como:
- Fraude de suscripción, que hemos visto anteriormente)
- Fraude interno: Personal de la operadora ayuda a los defraudadores
- Fraude técnico: Robo/Clonación de las tarjetas SIM
Las tarjetas se envían a otro país, donde los defraudadores los utilizan para llamar a números de tarificación adicional y cobran una cantidad por las llamadas recibidas, los usan en locutorios "clandestinos" y venden y/o hacen un uso abusivo de datos y servicios

-Fraude SIM Box /By Pass / Derivación de llamada. Una SIM Box que es un dispositivo que contiene múltiples tarjetas SIM.
Esta SIM Box puede utilizarse para recolectar y enrutar llamadas internacionales "saltando" la pasarela internacional, las llamadas internacionales entrantes no son enrutadas a través de la pasarela legítima y en su lugar son dirigidas a una pasarela privada ilegal (la SIM box operada por el defraudador) y posteriormente enrutadas a su destino como si fuese una llamada local evitando que la operadora pueda cobrar por esa comunicación



Esquema fraude Sim Box / By Pass

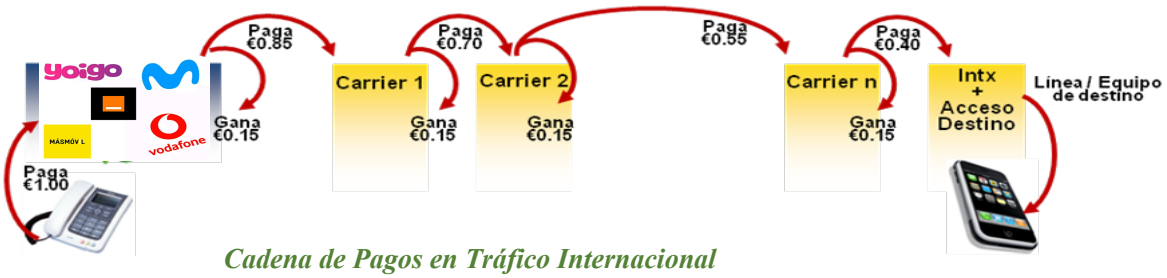


Dispositivo Sim Box

-Fraude IRSF (International Revenue Share Fraud)

En el momento que se inicia una llamada internacional, ésta va realizando saltos por carriers intermedios entre la red de acceso origen y la red de destino. El número de tránsitos o carriers internacionales varía en función del destino, del volumen de tráfico, etc…

El llamante paga el coste total de la llamada internacional y los operadores intermedios cobran parte del importe total por el uso de su red transfiriendo el resto, en cascada, al operador siguiente de la cadena.

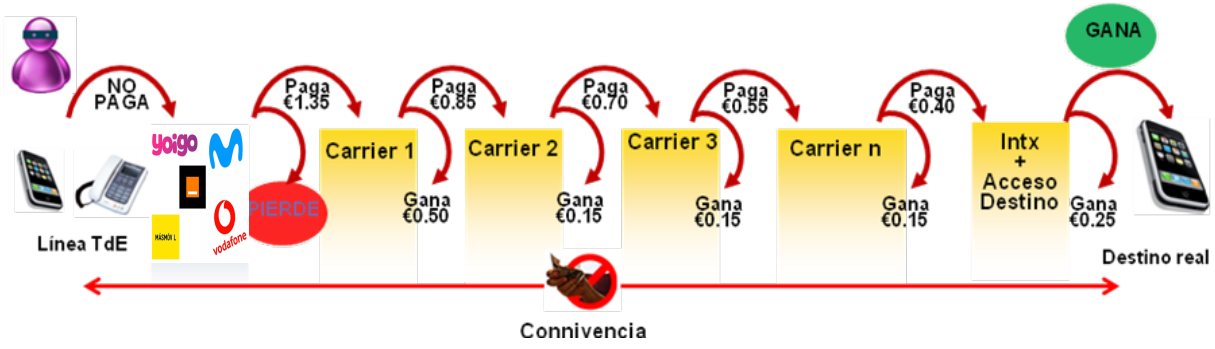


Cadena de Pagos en Tráfico Internacional

El International Revenue Share Fraud es un modelo de fraude que consiste en generar tráfico masivo a destinos internacionales. El titular de la numeración destino recibe del operador de acceso una parte del coste de la llamada por el tráfico que éste le genera. Este concepto se conoce como tráfico inducido consistente en buscar una descarga masiva de minutos para generar ingresos en el menor tiempo posible.

Para realizar este fraude se utilizan también SIM Box como las que hemos visto en el punto anterior, y fraudes como el **"Wangiri"** que impactan en el cliente y que veremos en el siguiente punto.

Las rutas hacia países con un alto importe de interconexión, desde la red de acceso origen del tráfico, suelen ser las más utilizadas en esta tipología de fraude por el alto coste (mayor beneficio para el defraudador) de las comunicaciones



Cadena de Pagos en IRSF

-Fraude "Wangiri", "one ring" o de la llamada perdida

Es una práctica telefónica fraudulenta en la que los defraudadores realizan múltiples llamadas por minuto a números escogidos al azar y corta de inmediato, lo que incita al destinatario a devolverlas. El objetivo es recaudar dinero cuando la víctima devuelve la llamada al tratarse de llamadas internacionales y/o a números premium de las que el defraudador obtiene beneficio.

En este caso el fraude no solo afecta a la operadora si no también al usuario que realiza la llamada

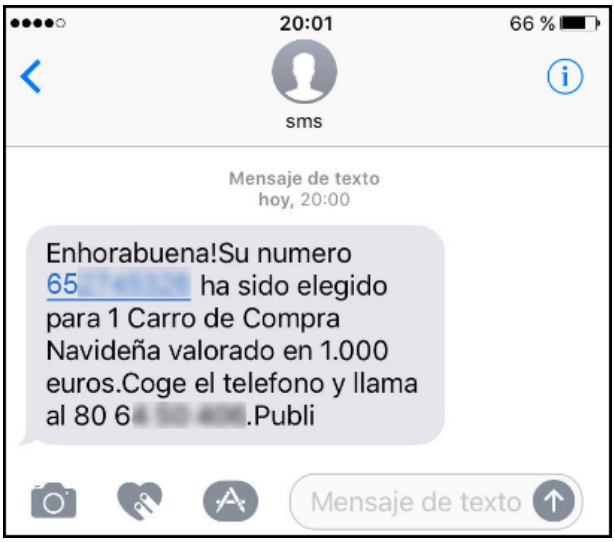
Además, los estafadores intentarán que la llamada tenga el mayor tiempo de duración posible para conseguir más dinero, esto lo consiguen introduciendo tiempos de espera, música, locuciones guiadas, etc…

-Fraude SMS

Aunque cada vez se utiliza menos el SMS, al menos en el ámbito personal, ya que las empresas siguen haciendo uso de ello, el fraude de SMS impacta tanto en la operadora como en el usuario

Tipos de fraude SMS

- Spaming SMS. Mensajes no deseados
- Phising Scam
  - Extorsión
  - Ingeniería social
  - Premium Rate Services (números de alta tarificación)
  - Virus
- Flooding SMS: Súbito aumento de mensajes en la red
- Faking SMS: envío de SMSs desde un SMSC ilegal (Short Message Service Center / Centro de Servicio de Mensajes Cortos)
- Spoofing SMS: manipulación del origen de envío



El impacto que este tipo de actuación fraudulenta tiene sobre la operadora y los clientes es muy variada, mala Imagen de la operadora, fuga de clientes, problemas con clientes víctimas (engaños, extorsión), pérdida financiera para la operadora y pérdida financiera para el cliente, aumento de la carga y congestión de la red, …

-Fraude interno

Es, como resulta obvio, el fraude realizado por los empleados, subcontratados, distribuidores, …. En la mayoría de los casos no actúan solos y suelen ser meros facilitadores a cambio de una compensación y en casos menos frecuentes, de forma no deliberada y debido a una extorsión, chantaje, etc...

Por lo general los métodos utilizados en este tipo de fraudes es la manipulación de los equipos de red dando acceso a los defraudadores, la manipulación y/o actuación sobre los sistemas de facturación, gestión de clientes, canales de venta, CRM, ….

Existen muchas más tipologías de fraude que además en muchos casos se combinan entre ellas, y seria muy extenso nombrarlas y dar una pequeña explicación de cada una de ellas, sólo quiero terminar este apartado del artículo, agrupando las técnicas de los defraudadores en tres grupos

- Relacionadas con consumo
  - Utilización de productos y servicios de la compañía.
- Relacionadas con equipamiento
  - Ataque de dispositivos
  - Utilizando herramientas para cometer el fraude.
- Relacionadas con las personas
  - Acción del defraudador sobre los clientes o los empleados.

El área de seguridad y el fraude

Bueno, pues vamos con el último punto que hemos nombrado en la introducción de este articulo y al que seguro que muchos estaban deseando llegar, ya que me atreví a utilizar el término "intrusismo" a sabiendas de que despertaría interés porque es algo que sufrimos y con el que todos en este sector estamos muy sensibilizados, aunque recuerden que también rápidamente maticé, que se trata realmente de una cuestión meramente organizativa, de responsabilidades y de intereses internos dentro de las empresas

Voy a compartir unos enlaces a las páginas de Interpol, de Europol y de la GSMA relacionadas con el fraude en telecomunicaciones

1.- Interpol: Reunión de expertos para luchar contra el fraude en telecomunicaciones y otras estafas

https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2019/Reunion-de-expertos-para-luchar-contra-el-fraude-en-telecomunicaciones-y-otras-estafas

> *"Los fraudes en telecomunicaciones y las estafas BEC* constituyen un grave motivo de preocupación para muchos países y tienen un efecto extremadamente dañino para los sistemas económicos, las empresas y la sociedad."*
>
> *Rory Corcoran*
>
> *Director del Centro de INTERPOL contra la Delincuencia Financiera y la Corrupción*

**Fraude/estafas BEC (Business Email Compromise) También conocido en España como Fraude del CEO*

2.- Europol creó el European Cibercrime Centre (EC3) y ha formado un grupo de trabajo donde participan operadoras de telecomunicaciones y empresas proveedoras de soluciones y servicios de prevención del fraude, para compartir información, recursos, y formación, y uno de los primeros fraudes sobre los que se ha trabajado ha sido el fraude IRSF del que hemos hablado anteriormente.

https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/telecommunications-fraud

3.- La GSMA (GSM Association, acrónimo de Global System for Mobile Communications) la principal asociación de telecomunicaciones reúne a más de 750 operadores de telefonía móvil de todo el mundo y más de 400 empresas relacionadas con el ecosistema móvil. Y entre sus grupos de trabajo está el FASG (Fraud and Security Group)

https://www.gsma.com/aboutus/workinggroups/fraud-security-group

También en este articulo lo primero que se ha reflejado es la definición de fraude según el Diccionario de la Real Academia Española, el código penal español y una de las principales operadoras de telecomunicaciones de España

Bien, ¿y todo esto por qué?; pues porque como hemos estado viendo, la prevención del fraude consiste fundamentalmente en luchar contra los delitos cometidos por personas o grupos organizados que tienen en su objetivo a la operadora o a sus clientes, utilizando las redes y servicios de la operadora para obtener un beneficio a costa de producirles un perjuicio económico.

La gestión de la prevención del fraude se debe definir bajo la premisa de la segregación de funciones y que pueda actuar con total independencia, por ello esta función debe estar **ligada al área de Seguridad** debido a la necesidad de investigación policial y judicial que conlleva el fraude ya que, **por su naturaleza, el fraude es un delito** como hemos visto en esas definiciones del inicio del artículo.

En muchas empresas, consultoras y asociaciones, abogan por distintas formulas para justificar quienes creen que deben ser los responsables de esta función de prevención del fraude, ya sea finanzas (control de gestión y aseguramiento de ingresos), gestión de riesgos operacionales, auditoria, …

El aseguramiento de ingresos tiene que ver con ajustes técnicos y operativos en los sistemas y procesos de negocio para evitar pérdidas de datos o actuaciones erróneas que dan lugar a lucro cesante. Se trata por tanto de una problemática de índole técnica y operativa que puede apoyarse, circunstancialmente, en la función de prevención del fraude y viceversa.
La gestión de riesgos tiene que ver con el crédito y confianza que se concede a los clientes para que adquieran y utilicen los productos y servicios y, en consecuencia, haya garantía del cobro acorde a las relaciones contractuales. Se trata de una problemática de índole comercial que necesita relacionarse con la función de prevención del fraude en lo referente a procesos internos y externos, pero ambas deben ser independientes.
La función de prevención del fraude en un operador de telecomunicaciones no es una actividad asimilable a la de aseguramiento de ingresos o la de gestión del riesgo. La única semejanza es el fin que todas ellas persiguen, evitar las pérdidas en el negocio. Por el contrario, son muchas las diferencias tanto en referente a los recursos como a los procesos y organizaciones involucradas en cada una de ellas.
Además, hay que tener en cuenta que, si se asocia esta función con la dirección financiera, una eventual deficiencia en la prevención del fraude podría interpretarse como mala práctica financiera, lo que afectaría además a la imagen de la empresa frente a los inversores y a su reputación corporativa

Obviamente, en todas las empresas las funciones y el alcance da las áreas que la conforman no son islas incomunicadas, todos los departamentos tienen una visión y una responsabilidad transversal y hay procedimientos y procesos que afectan a varias o a todas las áreas, pero la responsabilidad final y la gestión de la prevención del fraude, repito que ***debe estar ligada al área de Seguridad debido a las implicaciones tanto de investigación como judicial que conlleva el fraude*,** como también hemos visto con las

principales organizaciones policiales europea y mundial, y la principal asociación de telecomunicaciones móviles que unen ambos aspectos, seguridad y fraude.

Por último, y como cierre de este artículo, aunque todos nos la conocemos ya de memoria, no podemos obviar lo que dice el **articulo 36 de la Ley 5/14, de 14 de abril, de Seguridad Privada** y que copio aquí resaltando los puntos que evidencian y justifican que **en nuestro país la función de prevención del fraude debe recaer en el Director de Seguridad.**

Artículo 36. Directores de seguridad.
1. En relación con la empresa o entidad en la que presten sus servicios, corresponde a los directores de seguridad el ejercicio de las siguientes funciones:
a) La organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles.
b) La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio.
c) La planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables.
d) El control del funcionamiento y mantenimiento de los sistemas de seguridad privada.
e) La validación provisional, hasta la comprobación, en su caso, por parte de la Administración, de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada.
f) La comprobación de que los sistemas de seguridad privada instalados y las empresas de seguridad privada contratadas, cumplen con las exigencias de homologación de los organismos competentes.
g) La comunicación a las Fuerzas y Cuerpos de Seguridad competentes de las circunstancias o informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos de los que tenga conocimiento en el ejercicio de sus funciones.
h) La interlocución y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos.
i) Las comprobaciones de los aspectos necesarios sobre el personal que, por el ejercicio de las funciones encomendadas, precise acceder a áreas o informaciones, para garantizar la protección efectiva de su entidad, empresa o grupo empresarial.

Luis Miguel Hurtado Zabaleta
Director de Seguridad
www.linkedin.com/in/luis-miguel-hurtado