
# CSG FRAUD PROTECTION

## IDENTIFICAR E ERRADICAR FRAUDES

Fraudes constituem um grande problema para operadoras de rede móvel (mobile network operators, MNOs) em todo o mundo, com um custo de mais de US$ 38 bilhões anualmente. Mas entre todos os problemas de fraude de interconexão, o “bypass” ilegal é de longe o maior. Em muitos países, a tarifa da terminação internacional (international termination rate, ITR) é consideravelmente maior que a tarifa da terminação local (varejo) para um número de celular no país. Isso faz com que seja lucrativo para os fraudadores contornar a operadora internacional licenciada ao terminar chamadas no país. Desta forma, eles pagam a tarifa inferior da terminação local, em vez da ITR. Esta prática é ilegal na maioria dos países e é um grande problema para várias operadoras devido às receitas perdidas.

## COMO FUNCIONA A FRAUDE DE BYPASS ILEGAL

A forma mais simples de cometer fraude de bypass ilegal envolve configurar uma SIM Box (gateway GSM). Os equipamentos padrão podem ser facilmente adquiridos na Internet, e equipados com um conjunto de cartões SIM. As chamadas são normalmente redirecionadas por meio de uma conexão com a Internet para uma SIM Box localizada no país de destino. Assim, a SIM Box converte a chamada em uma chamada de celular para o destinatário na rede móvel.

Outra variante do bypass ilegal é quando equipamentos de linha fixa, como um “leaky PBX”, são usados para converter a chamada em uma chamada local. Isso é menos comum do que as SIM Box, mas também constitui um problema significativo para as operadoras.

## A DIMENSÃO DAS FRAUDES DE SIM BOX

A “terminação de SIM Box” de chamadas internacionais entrantes, também conhecida como “fraude de bypass de operadora,” é um grande problema para operadoras de rede móvel e operadoras de gateway internacional (international gateway operators, IGW) licenciadas. Isso resulta em uma má experiência para o cliente e consequente “churn,” bem como perda de receitas. Em alguns países, até 70 por cento das chamadas internacionais recebidas são terminadas de forma fraudulenta. A Communications Fraud Control Association (CFCA) estima que US$ 6 bilhões são perdidos anualmente apenas com a fraude de bypass de interconexão. Isso não só afeta as operadoras, mas também as autoridades fiscais dos países afetados, já que os impostos sobre tráfego internacional não podem ser cobrados.

© 2018 CSG SYSTEMS INTERNATIONAL, INC. AND/OR ITS AFFILIATES (“CSG”). ALL RIGHTS RESERVED.

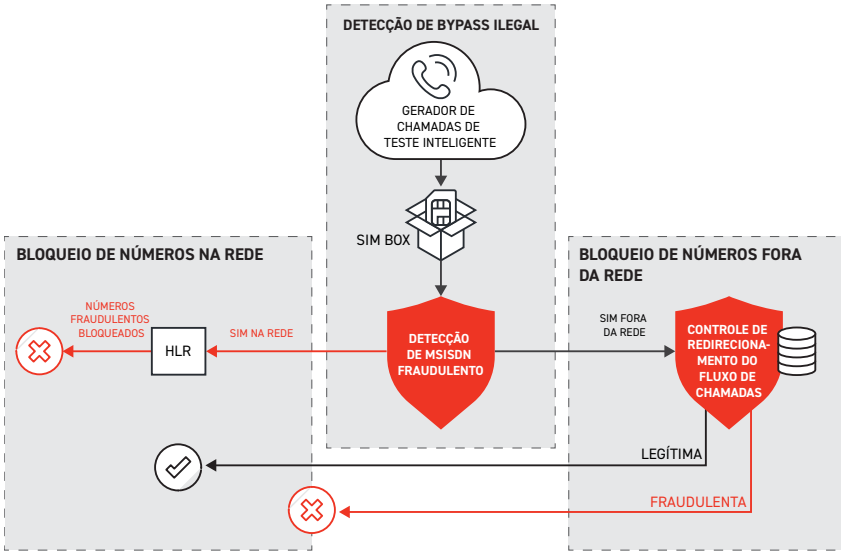
## AS CONSEQUÊNCIAS DA FRAUDE DE BYPASS ILEGAL

- **Perda direta de receita**
  - Em vários casos as operadoras perdem centenas de milhares de dólares por mês
- **Perda indireta de receita**
  - Identificação de chamadas (Calling Line Identifier, CLI) ausente ou incorreto, o que significa que muitas chamadas são rejeitadas pelo destinatário (assinante B) e que as chamadas perdidas não são retornadas. Isso resulta em ainda mais perdas de receitas para as operadoras
  - Degradação na qualidade de voz devido a problemas de latência, conexões IP altamente compactadas e maior tempo de completamento da chamada. Isso afeta a experiência do cliente e a reputação de ambas as operadoras. A experiência do cliente tem um impacto direto na fidelidade e em seu gasto mensal pelo tempo que segue como cliente

## PROTEÇÃO CONTRA FRAUDE DA CSG: DETECÇÃO DE BYPASS ILEGAL COM BLOQUEIO AUTOMÁTICO

A CSG fornece soluções de OSS e BSS a centenas de operadoras em todo o mundo, concebidas com base em informações exclusivas para criar uma solução de Proteção Contra Fraudes abrangente e totalmente integrada.

A solução permite em primeira instância localizar um número de SIM Box em uma única chamada. Esta abordagem com base em chamadas de teste tem a vantagem de ser rapidamente executada, que é essencial para identificar atividades fraudulentas na rede. Assim que os números da SIM Box são identificados, a solução de Proteção Contra Fraude da CSG permite bloquear automaticamente os números em rede descobertos e as chamadas fora da rede de números identificados da SIM Box. A integração ponta a ponta é parte essencial do desenho da solução, permitindo que a funcionalidade de bloqueio automático supere a velocidade com que os cartões SIM utilizados de forma fraudulenta são substituídos. A CSG acredita que uma abordagem manual ao bloqueio de cartões SIM não é relevante e não é eficaz o suficiente contra operações fraudulentas altamente sofisticadas.




© 2018 CSG SYSTEMS INTERNATIONAL, INC. AND/OR ITS AFFILIATES ("CSG"). ALL RIGHTS RESERVED.

# OS RECURSOS DA SOLUÇÃO

Em alto nível, os recursos da solução incluem:

- Serviço de classe mundial para detectar SIM Boxes ativas
- Controle de fluxo de chamadas a nível do software em vez de soluções à base de sondagem, que são vulneráveis a fraudes internas e exigem manutenção de hardware significativa
- Bloqueio em tempo quase real de números de SIM Boxes em rede detectados
- Bloqueio em tempo quase real de chamadas de números fora da rede detectados
- Capacidade de bloquear números manualmente a nível granular (por endereço IP, porta, SIP/TDM, etc.)
- Capacidade de desbloquear números manualmente
- Capacidade de gerar relatórios
- Projeto concebido para agregar valor o mais rapidamente possível

© 2018 CSG SYSTEMS INTERNATIONAL, INC. AND/OR ITS AFFILIATES ("CSG"). ALL RIGHTS RESERVED.