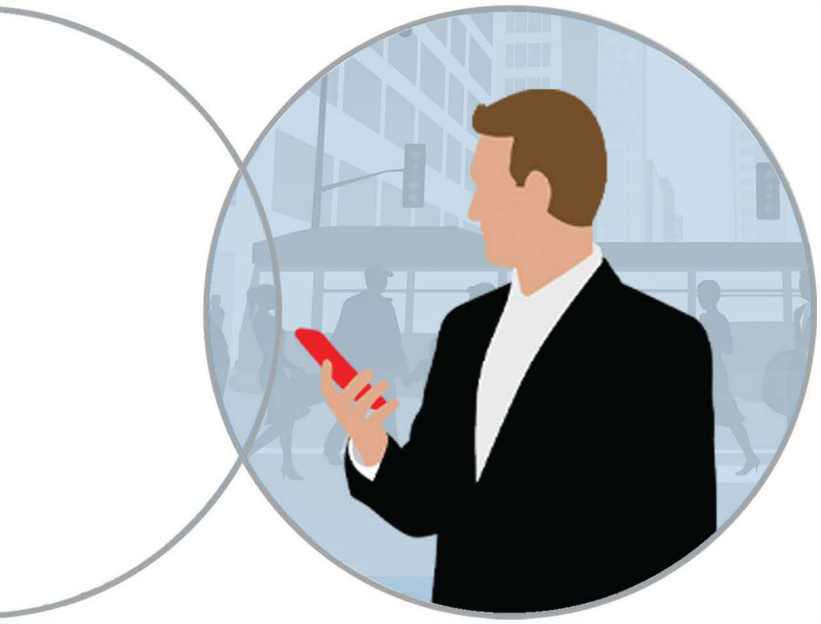
stop telecom fraudsters in their tracks

the cost of telecom fraud

Service providers continue to struggle with significant telecom fraud losses despite having implemented sophisticated revenue assurance processes and fraud management systems.

Fraud totaled $39.89 billion in 2021, according to the Communications Fraud Association (CFCA). That is 2.22% of global telecom revenues. This makes fraud a more than 10 billion U.S. dollar-a-year problem and it could be as high as 40 billion U.S. dollars annually, according to the Communications Fraud Control Association (CFCA).



how global numbering data can help

There are encouraging signs that a more holistic approach to fighting International Revenue Share Fraud (IRSF) including PBX hacking fraud is gaining traction among service providers.

Service providers can now use detailed number plan data as a complement to their traditional fraud management systems to:

- Proactively identify and block fraudulent calls to high-risk numbers
- Obtain early warnings for their fraud prevention teams on impending attacks
- Stop future fraud rather than relying on blacklists associated with past fraud events

stop telecom fraudsters in their tracks

how IRSF fraud is committed

Typically, fraudsters exploit telephone numbers with high termination rates, from which they obtain a revenue share, including international revenue share and premium rate services provided by third parties. By generating large volumes of traffic to these high-risk numbers in a short period of time, fraudsters can make substantial profits before a service provider's fraud management system is able to detect the fraud and shut down the service.

The fraudsters have obviously no intention of paying for these expensive calls. They typically use stolen credit cards or commit identity theft to gain access to the service. Some even use stolen mobile phones or SIM cards. The fraud attacks typically happen outside of normal business hours and often while the subscriber is roaming, which delays and complicates the process of detecting and stopping the fraud.

The charges generated by a single fraud incident can vary from a thousand U.S. dollars up to hundreds of thousands of U.S. dollars, depending on the sophistication of the attack and how quickly the fraud team can respond.

A similar illegal revenue-generating scheme is PBX hacking, where fraudsters hack into an enterprise phone system and start making outgoing calls to expensive international revenue share numbers. A single incident can result in a five- or six-figure loss to the service provider, as the enterprise customer will often refuse to pay the amount.

In addition to revenue share and premium rate numbers, fraudsters take advantage of unallocated numbers (i.e. number ranges that are not yet in use) and illegally re-route the numbers to existing international premium rate services, typically via a transit service provider. This introduces an additional level of complexity to fraud prevention, generating further revenue loss for service providers and enterprises.

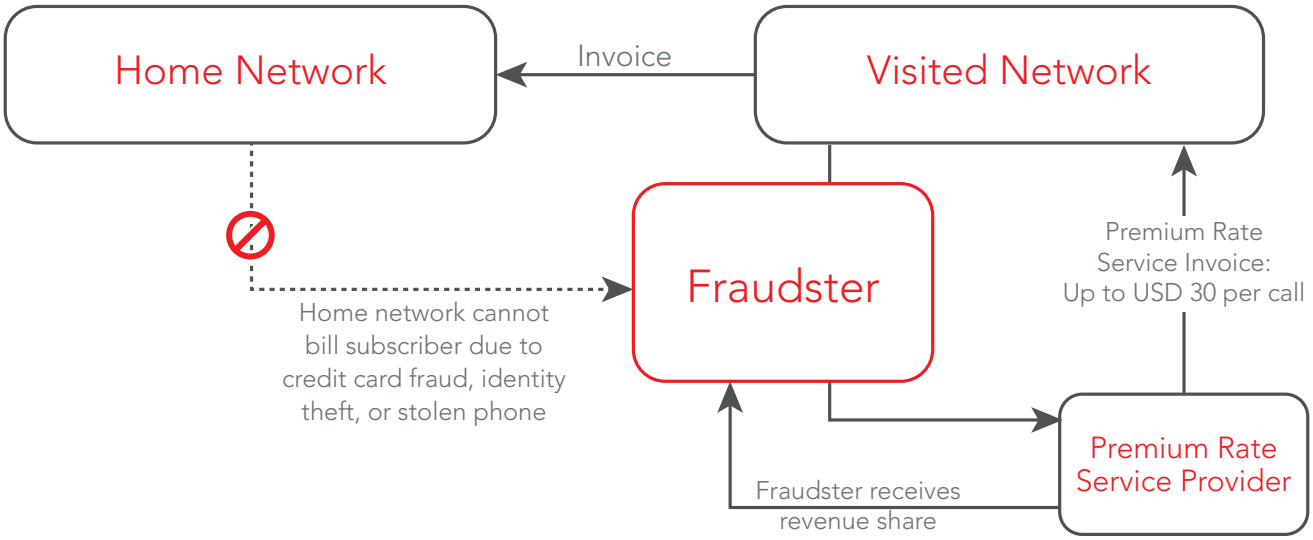


Figure 1: A typical scenario involving fraudulent roaming calls to a premium rate service. The Premium Rate Service Provider sends a bill to the Visited Network, which pays it and then invoices the Home Network, which will eventually be stuck with the bill due to the fraud committed. The Premium Rate Service Provider finally pays the fraudster a revenue share

stop telecom fraudsters in their tracks

benefits of accurate numbering information

To improve fraud prevention efficiency and minimize fraud losses, service providers are starting to use new sets of numbering information as a complement to their existing fraud management systems.

Service providers can now utilize detailed number range data from countries across the globe including a comprehensive list of high-risk revenue share, premium rate and unallocated number ranges. These data sets enable service providers to effectively pinpoint and flag potential fraudulent calls and take immediate preventive action before completion of such identified calls.

how global number range information works

Take, for example, the case of a European incumbent who was encountering significant fraud in its mobile, fixed and wholesale business units, particularly from PBX hacking. Despite continuous investments in traditional anti-fraud solutions, the service provider was not able to control its losses. It eventually concluded that it had no choice but to change its approach and decided to implement a solution that leveraged global number range information. The results exceeded expectations:

- Dramatically reduced fraud losses with minimal level of customer complaints
- Achieved zero losses from PBX hacking attempts
- Improved customer satisfaction for enterprise customers

requirements and implementation

Improving fraud protection by leveraging global number range information is a straightforward task but it does require the introduction of some new processes and, of course, access to accurate and detailed global number range data. As service providers adopt this new approach to fraud prevention, they should consider the following best practices[3]:

- Obtain comprehensive numbering information that includes a list of high-risk revenue share, premium rate and unallocated ranges
- Use of real-time call control and dialed number query against a database of high-risk numbers
- Real-time alarming and reporting of all blocked calls
- Use of a web-based GUI that gives fraud managers greater insight and control
- Development of an allow list containing validated premium rate service numbers

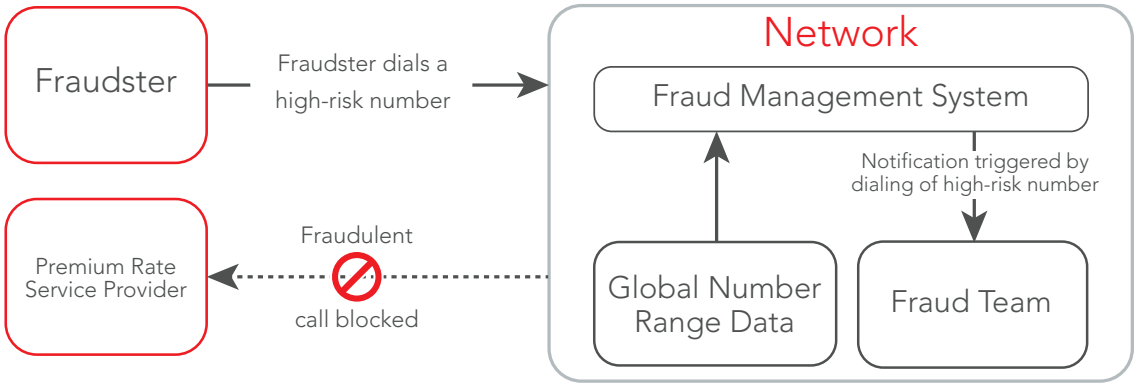


Figure 2: Proactive blocking of a fraudulent call to a high-risk number using a global number range database, which contains detailed information on premium rate service and unallocated number ranges

putting it all together

While telecom fraud continues to deteriorate profit margins, service providers are starting to adopt a more comprehensive approach involving the use of accurate and detailed global number range information to complement existing fraud management systems.

This approach requires global numbering information procured from authoritative sources with the following features:

- Data procured from authoritative sources within respective countries on allocated and unallocated number ranges
- Comprehensive information on high-risk revenue share, premium rate services compiled and offered through a single source
- Continuously updated number ranges with information on which service providers they belong to

Moving to a proactive fraud prevention strategy rather than relying solely on reactive detection and blacklists of numbers involved in past fraud incidents provides significant benefits and ROI, such as:

- Immediate blocking of fraudulent calls to high-risk numbers, including unallocated and premium rate numbers
- Early warnings to the fraud prevention team whenever a high-risk number is being dialed
- More efficient use of fraud prevention team resources

let's talk about your fraud prevention needs

iconectiv® has been the leader in numbering management and authoritative telecom database solutions for more than 30 years, iconectiv has frequently contributing to industry organizations committed to fighting telecom fraud, including the GSMA Fraud and Security Group and the CFCA.

Please contact us to learn more about how you can become more proactive in fighting IRSF and PBX hacking fraud.

FOOTNOTES

1 https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf

2 https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf

3 While not all of the outlined steps are strictly required, it is the recommended approach to maximize fraud protection

about iconectiv

Your business and your customers need to confidently access and exchange information simply, seamlessly and securely. iconectiv's extensive experience in information services, digital identity and numbering intelligence helps you do just that. In fact, more than 5K customers rely on our data exchange platforms each day to keep their networks, devices and applications connected and 2B consumers and businesses protected. Our cloud-based information as a service network and operations management and numbering solutions span trusted communications, digital identity management and fraud prevention. For more information, visit www.iconectiv.com. Follow us on X and LinkedIn.

make the connection.

For more information about iconectiv, contact your local account executive, or you can reach us at:

+1 732.699.6800

info@iconectiv.com

www.iconectiv.com