# Q2 2016 Fraud Report from SmartIPX

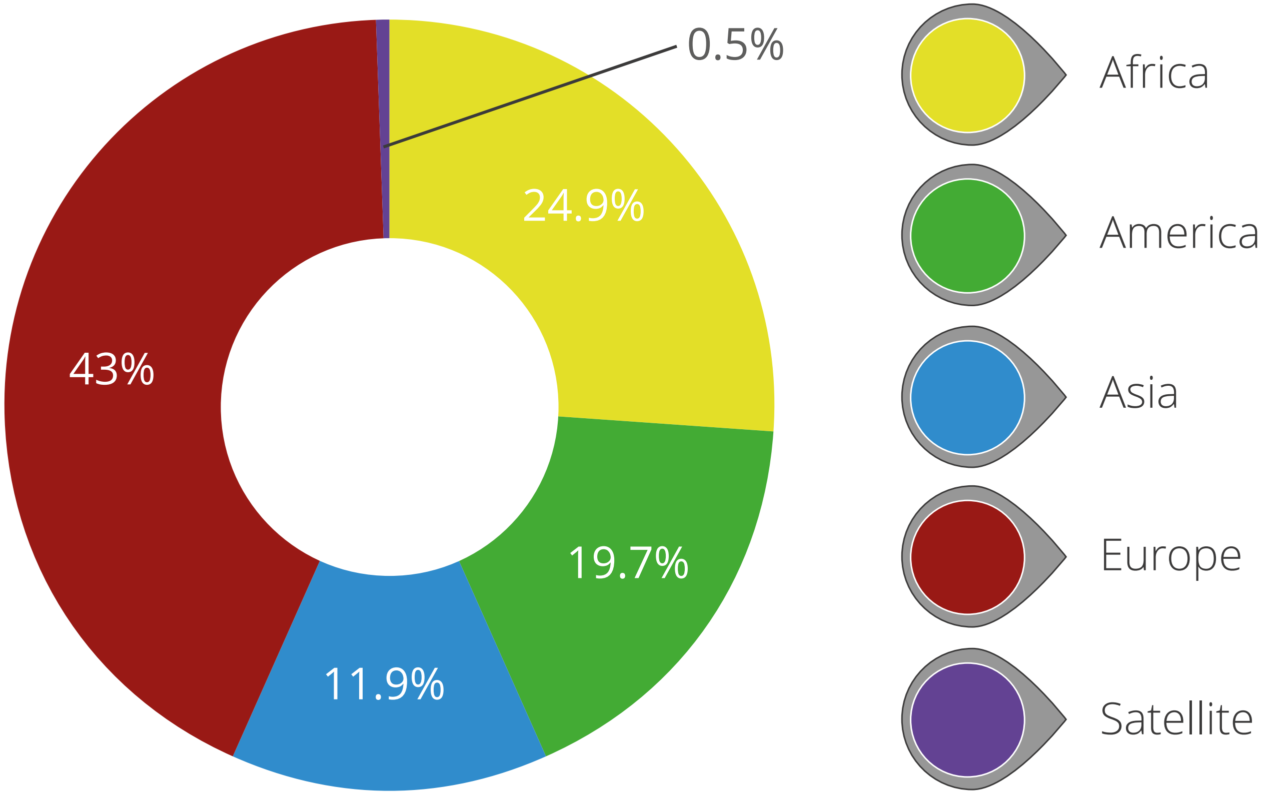
South America and Caribbean number ranges back in fashion

# The developing global fraud landscape in 2016

Telecoms fraud is present across the globe. There isn't a continent which doesn't have some element of fraudulent activity either originating or terminating in that part of the world.

Traditionally, Africa was seen as a common target for telecom fraud, because the termination costs are very high and regulation is not as stringent as in other parts of the world. During 2015 and the early part of 2016, the focus for the termination of fraud shifted to Europe, specifically within the Balkan States like Bosnia, Serbia, Azerbaijan and Albania. However, whilst these destinations remain the most active, during the second quarter of 2016 there has been a rise in fraud attempts using South America and the Caribbean specifically around Haiti, the Cayman Islands, Dominica and St Kitts & Nevis, with other new destinations including Eritrea, Morocco, Bolivia and Latvia.

## Profile of VOIP wholesale fraud destinations



Whether this further shift denotes a permanent strategy by the fraudsters and criminal gangs perpetrating this activity, we will learn more as 2016 progresses and will report further upon in our Q3 and Q4 guides.

However, we can be certain that staying one step ahead of fraudsters remains a challenge with increasing sophistication on both sides due to substantial and increasing rewards for those who commit these crimes, and substantial risks, financial and reputational, for those being defrauded.

# Cybercrime - including telecoms fraud - now more lucrative than narcotics

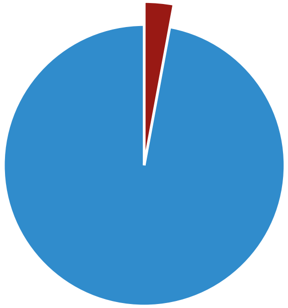
Telecom fraud is a lucrative criminal business and an attractive target for fraudsters. At the i3 forum's 7th annual conference last May, Robert Benlolo of Tata Communications, highlighted the financial implications of telecoms fraud in a stark presentation. Of the total $2.25 trillion of global telecom revenue, a staggering $38.1bn is lost to fraud annually - a 2% revenue loss across the industry as a whole.

**$2.25tn**

Global Telecom Revenue

**$38.1bn**

Amount lost annually to fraud



**2%**

Global telecom industry revenue loss

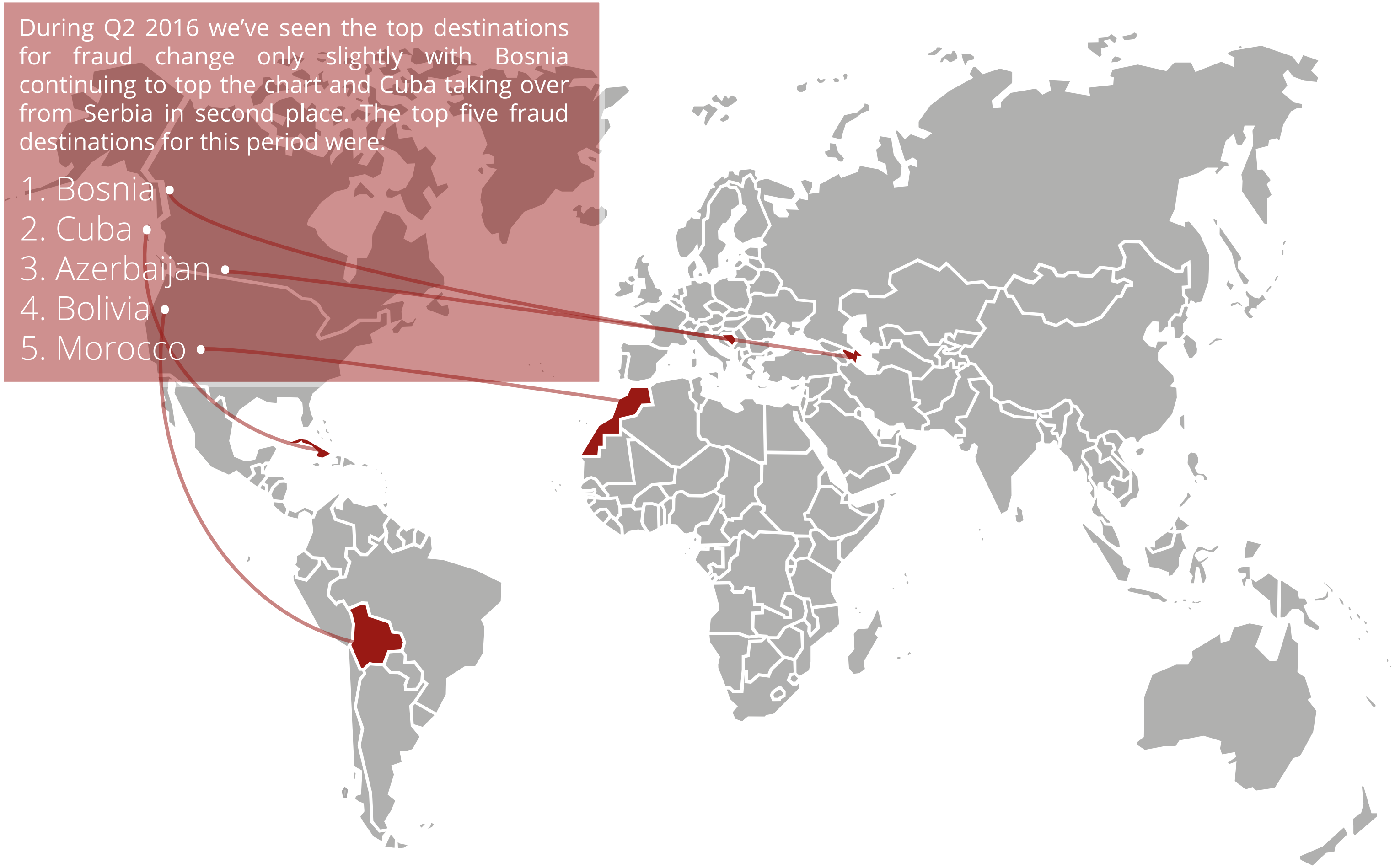
In China, a series of telecoms frauds nationwide netted $3.3bn while in February this year a former Pakistani national was sentenced by a US court after he admitted laundering more than $19.6m in support of a massive international computer and telecommunications fraud scheme.

Europol believes that cybercrime is now more lucrative than the narcotics trade for criminal cartels and it's considered to be far safer. In its 2013 Europol Serious & Organized Threat Assessment, Europol reported: "The Total Global Impact of CyberCrime [has risen to] US $3 Trillion, **making it more profitable than the global trade in marijuana, cocaine and heroin combined**."

The impact of this fraud goes beyond the pure financial impact however, with China Daily reporting in its May US edition of a growing number of suicides being linked to targeted telecoms fraud.

Speaking in 2015 former City of London Police Commissioner Adrian Leppard said at least a quarter of organised criminals in Britain were now involved in online fraud of some kind. International gangsters were increasingly abandoning drug dealing and other high risk rackets in favour of cybercrime.

# The geography of fraud



During Q2 2016 we've seen the top destinations for fraud change only slightly with Bosnia continuing to top the chart and Cuba taking over from Serbia in second place. The top five fraud destinations for this period were:

1. Bosnia •
2. Cuba •
3. Azerbaijan •
4. Bolivia •
5. Morocco •

Below the top 5, there has been an increase this quarter in the number of fraud attempts and attacks from South America and the Caribbean. Overall, the Americas region rose from 20% to 37% of all fraud traffic in the first quarter of 2016. Haiti saw the highest increase, up from 1% to 5% during the last three months.

These findings show a progressive change from those in the 2015 Communications Fraud Control Association report[1], which shows the top five countries where fraudulent calls terminate as:

1. Cuba
2. Somalia
3. Bosnia & Herzegovina
4. Estonia
5. Latvia

[1] *CCFA reports at a regional level; our reporting reviews quarter on quarter information from within our customer base.*

# The timing of fraudulent attacks

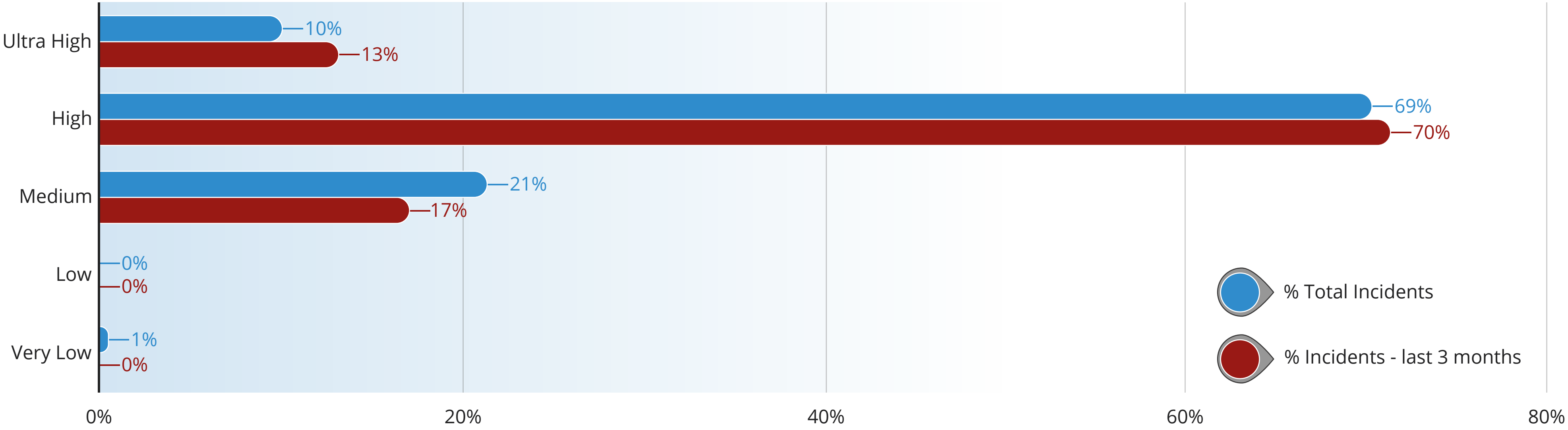
Most attacks still take place towards the end of the working week due to the higher chances of fraud going undetected outside of the normal trading hours of 9 - 5 Monday to Friday, in our case CET.

Attacks out of these normal trading hours have risen to account for 90% of all incidents in the past three months, with 40% now taking place at the weekend, a rise from 33% in the previous quarter.

Friday continues to be the most popular day for an attack to start, with 50% taking place on that day in Q2 2016,  but Sunday has seen an increase in fraudulent activity rise from 11% to 27%.

In addition to these changes to attack timings, there has also been a rise in the value of the targets being attacked, with the Fraud Incidents by Rate Value Risk Group (%) figures reflecting this change.

## Fraud incidents by Rate Value Risk Group (%)



Both High and Ultra High value risk groups have seen increases in fraud attacks and attempts during the second quarter of the year and as a result of this increasing trend, changes have been made to the monitoring algorithms to help identify such attempts before they happen[1].
As a result of intelligent monitoring,  Latvian number ranges have been added as an Ultra High value risk destination due to the termination cost of calls (+£0.70) which can be five to seven times more expensive than within the EU.

[1] *Ultra High and High value risk groups are those where the termination destinations are most exposed to fraud. There are usually higher costs incurred in calling to these locations.*

# How to combat telecoms fraud

Combating fraud is an ongoing battle for the telecoms industry worldwide with technologies and methodologies advancing all the time on both sides.

While the primary way to combat telecoms fraud is to make sure you know what it is and how it can occur, service providers and operators are already developing a variety of robust and responsive monitoring systems to help identify, minimise and contain threats as they arise. This is done through a combination of collaboration between service providers and through vehicles like the i3 Forum. It helps develop and maintain trusted relationships with customers.

The primary way to combat telecoms fraud is to make sure you know exactly what it is and how it can occur: preparation requires perfect planning and the perfect technical & operations partner.  Fraud is a threat to all operators, wherever they are located and whatever their size. To the more vulnerable, it could even be the difference between survival and insolvency. It certainly won't do any good to an operator's reputation and image to be identified as a fraud victim.

The challenge is to identify fraud as it changes and evolves. Criminals are innovative and are continually finding new ways to elude operators. While there are a range of different schemes and scenarios where fraud occurs, there are also a few common types of fraud like:

## PBX Hacking/IP PBX Hacking

An enterprise PBX is hacked, creating an opening for several types of fraud. A hacker might use out of office hours to make multiple calls to premium destinations, sharing the revenue with the terminating end.

## False Answer Supervision

This can either involve triggering switches to start the billing process in, favoring one interconnect wrongfully, even though end subscriber hasn't answer the call yet. Or a call can be hijacked and transferred to an IVR system preventing the caller from reaching the intended destination and still charging the subscriber for a service he did not get. This is now a must have capability to protect margin and quality control on routes to Africa destinations

## Wangiri Fraud

The fraudster automatically robot dials thousands of mobile numbers, terminating the call after one ring. This will prompt the unaware called subscribers to call back and being lured into a premium rate number which can cost as high as 15 USD per minute.
This is a growing problem on traffic terminating in Asia and Africa regions for all parties

## International Revenue Share

This fraud takes advantage of international destinations where termination comes at a premium rate. Either by use of a fraudulent SIM at the originating end of the call or a colluding third party at the termination end, these high rates can be exploited.

The “signature” of each fraud type is reflected in network behaviour, which can be identified with a combination of new network intelligence backed up by a responsive network team with the skills and experience to react appropriately in a timely fashion. A data-driven approach has been proven to work, whereby sophisticated Big Data analytics helps the service provider keep pace with evolving fraud techniques.

Network data and analytics captured by a next generation session border controller (SBC) can be positioned to work to not just optimise network performance, but also to identify and mitigate fraud.

Sitting directly in the call path, the SBC has the ability to capture data in real time and alert the service provider of any abnormal behaviours on the network and in individual sessions. Voice quality (MOS, R-Factor), Real Time Protocol Analysis (One-Way & Two-Way RTP, Set-up & Disconnect Time Stamping) and call behaviour (automatic speech recognition, call distribution, post dial delay) can all be examined to determine fraud in real time.

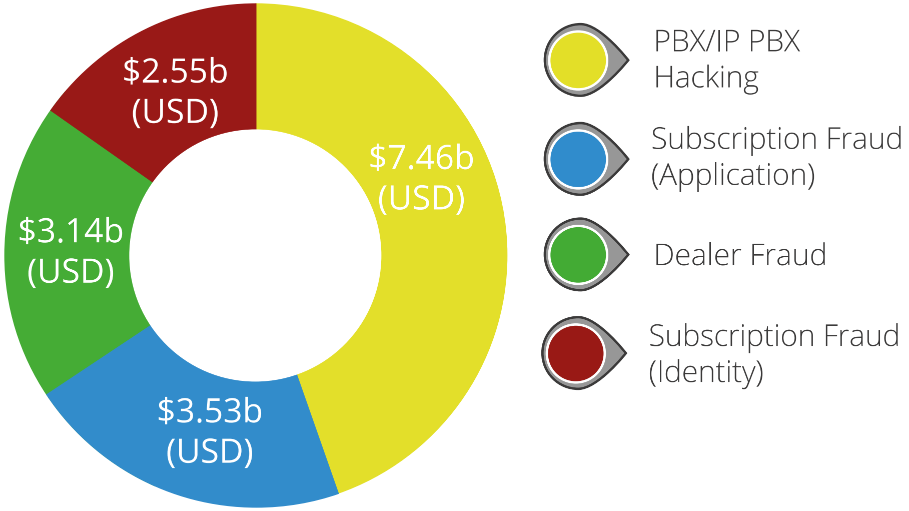
# Fraud can wipe out margins

As an industry combating fraud has reduced global revenue loss to criminals from 4% to 2%. Irrespective of brand protection, annually this is delivering 38 billion USD of benefits on existing business.

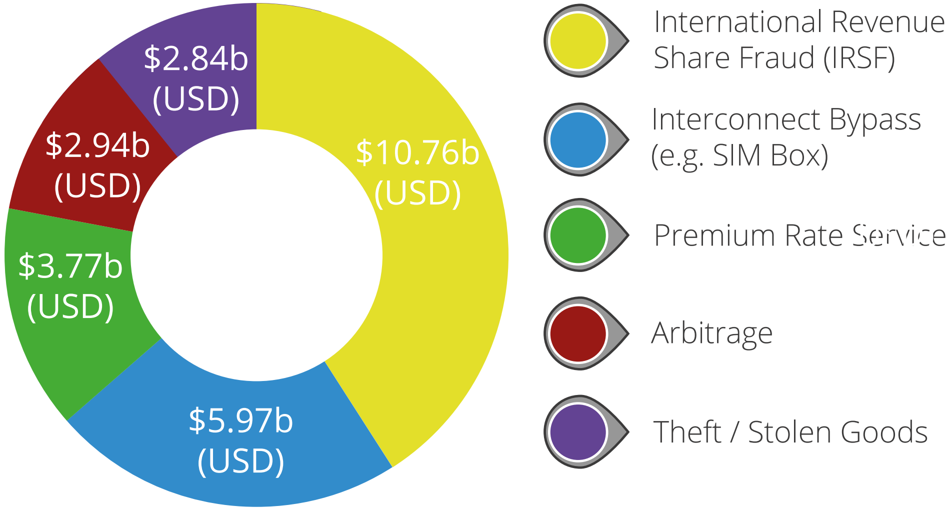
Typically an “in country” business Service Provider’s international calls represent less than 2 to 4% of their total minute volume, yet fraud can wipe out total monthly call margins and cause untold damage to their brand’s reputation.

Our research shows that wholesale partners are twice as likely to be attacked as retail only service providers and the benchmark margin cost per incident between 5k-10k USD depending on your sector.

**According to the CFCA 2015 Global Telecoms Fraud Survey the top four methods for committing fraud are:**



**And the top five types of fraud are:**



# Conclusion

Fraud tactics continue to adapt to the technologies and strategies put in place to combat them. There are different characteristics to each method of fraud and that is what makes them so challenging to identify. The variations evolve and change over time which is why new network intelligence and machine-learning are so crucial in the fight against fraud, working best when backed up with an experienced NOC team.

Due to the role they play in the network, next generation Session Border Controllers (SBCs) provide a deep analysis of signalling and media and offer unparalleled visibility. Compared to third party solutions or a solution that sits outside of the network, the SBC offers an immediate response with the added efficiency of using data that is available in the network. At SmartIPX we deploy Cataleya's Orchid One Network Session and Application Manager, (a highly advanced evolution of a Session Border Controller), on behalf of our clients.

A good SBC, backed up with thought through, well executed and regularly updated fraud mitigation plan will continue to be the best way to stay ahead of fraud and to ensure that losses are kept to a minimum. At SmartIPX, we will continue to build our team and implement the best technologies to protect our customers from the ravages of fraud, staying ahead of the game.

We hope you've found our Q2 Fraud Report useful. Please join the conversation on Twitter by using the hashtag "#CombatTelcoFraud" and follow @smartIPX for regular updates between our full quarterly reports.

Our Q3 Fraud Report will be published mid October and announced across our social media channels - if you would like us to consider anything for inclusion, please contact us via Twitter or on the contact page of our web site. Thank you.

## Sources

1. http://www.cfca.org/pdf/survey/2015_CFCA_Global_Fraud_Loss_Survey_Press_Release.pdf
2. http://www.cataleya.com/resources/blogs/fighting-voice-fraud-with-big-data-analytics/
3. https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015
4. https://www.europol.europa.eu/iocta/2015/
5. http://usa.chinadaily.com.cn/china/2016-06/15/content_25717351.htm

# SmartIPX helps customers prevent loss from fraud

SmartIPX helps assure voice margins in wholesale, retail and enterprise network environments.
Since the 2013 Communications Fraud Control Association survey, the number of respondents outsourcing some or all of their fraud management services has risen from 15% to 50%. Outsourcing helps companies avoid the massive capex of setting up and managing a fraud detection team 24*7.

Contact us to find out how SmartIPX have been successful in:

- Developing a sophisticated arsenal of tools/systems
- Evolved streamlined fraud management processes
- Invested in our highly proficient and expert NOC team (continuous training)
- Collaborative partner activity to improve performance

If you have not yet made the decision to get help with you fraud management, **or you are unhappy with your current solution performance**, contact...