FRAUD – LOCK DOWN!

HOT TELECOM
Research • Consulting • People

SPONSORED BY

telarix

Table of Content

OVERVIEW - FRAUD IS EVERYWHERE

It is hard to escape the fact that every element of our lives today are potentially subject to fraud. Technology, which provides often essential capabilities, is constantly being tested for weaknesses that can provide someone somewhere with the ability to make money without earning it. So why should the highly complex interconnected environment comprising the global telecoms network be any different?

Of course, it isn't. For example, the Communications Fraud Control Association (CFCA) estimates 2015's losses from telecoms fraud to be US$38.1 billion. If there is any good news in that massive number, it is that it is down by 18% since 2013, mainly because of more advanced fraud management solutions being offered by a few key industry vendors. The actual loss from fraud often is borne by the retail service provider and, for many years, wholesalers turned somewhat of a blind eye towards international revenue share fraud, where illicitly generated calls are routed to a distant, and expensive, international destination. The thinking was: We are correctly terminating calls that we have been asked to route and are charging the rate agreed, what is wrong with that?

However, the cut-throat competition in international voice is creating a new wave of interest in fraud mitigation. Carriers are starting to see value in helping their retail service provider customers mitigate the impact of fraud on their bottom line. Those carriers that can clearly help their customers minimize their own fraud issues will in return be seen as a valuable and long term partners, no longer fighting for traffic based on a marginally lower termination price, but providing a safe passage for calls without the risk of hijacking, false answers, or mobile operator bypass.

This white paper provides an overview of the sort of frauds increasingly hitting international carriers and what they can, and should be doing now to arrest it. We also discuss what tools are available to effectively and automatically provide much needed support to that task. Finally, we look into the future to see how fraud may evolve and what this may mean for the different telecom players going forward.

Steve Heap
CTO, HOT TELECOM

KEY MESSAGES

- ✓ Fraud mainly impacts retail service providers and end users
- ✓ Wholesalers have a key role to play in fraud management and detection to protect customers
- ✓ Fraud management done properly can enhance the reputation and success of wholesalers
- ✓ Advanced statistical analytics are critical allowing use of forecasting and predictive modelling
- ✓ Integration of best of breed components can provide the ideal fraud management environment
- ✓ Use of visualization can identify complex patterns and variations in call scenarios
- ✓ Automated link to routing control to block fraudulent calls improves efficiency

FRAUD 101

Telecom fraud is big business! The September 2015 survey published by the CFCA showed that fraud represents somewhere between 2% to 5% of global revenue - a colossal sum!

But how do those frauds take place? To be effective, a fraud requires two things:

1. A way to make calls (or generate texts) without paying for them
2. A way to take cash out of the telecom environment

In each fraud type, we often find that criminals identify the most efficient ways to extract money from a telecom service and then come up with endless ways to innovate around the methods of driving traffic to that service.

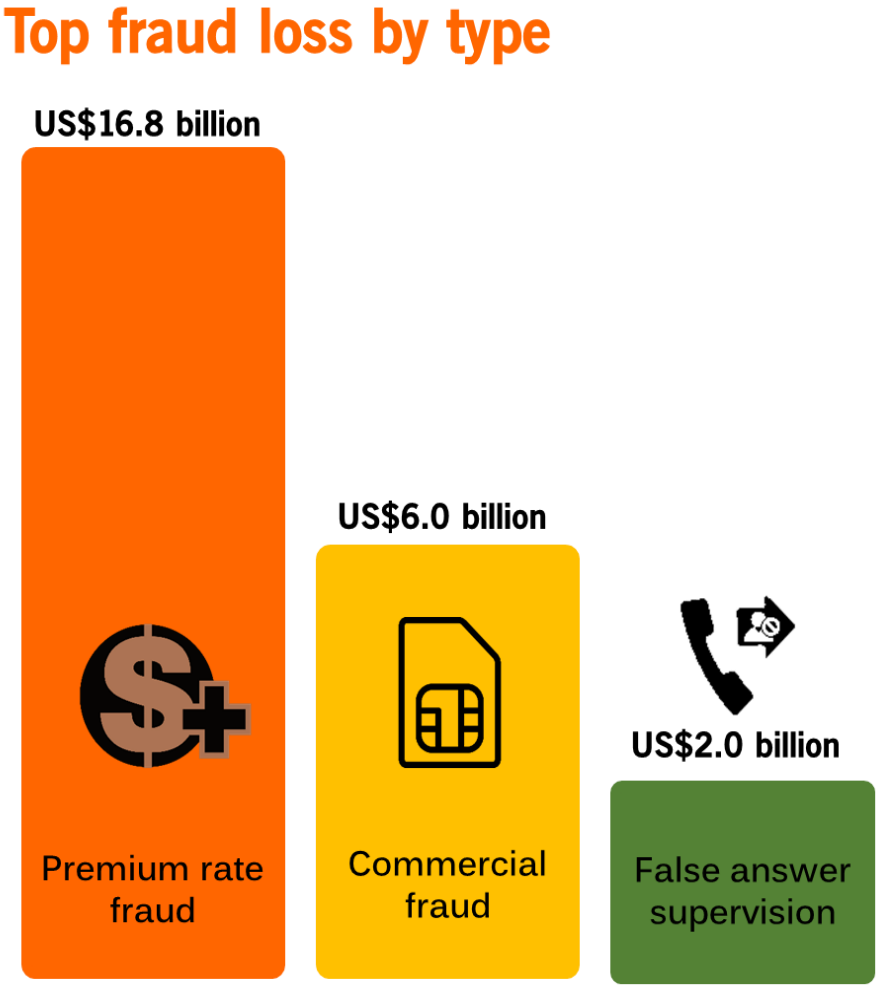
In general, four main categories of fraud can be identified, each of them using a different approach to gaining access to the monetary rewards:

1. Premium number fraud
2. Commercial fraud
3. False Answer Supervision
4. VAT fraud

Premium number fraud, often known as International Revenue Share Fraud (IRSF) alone represented almost US$14.6 billion of losses with domestic premium services adding US$2.2 billion to this.

Commercial frauds, which include regulated interconnect bypass, primarily using SIM boxes, hit retailers with a further US$6.0 billion of losses and this survey was taken before the mobile operator type bypass arrangements were fully implemented.

General wholesale fraud including False Answer Supervision added a further US$2.0 billion to the total. Although outside the focus of the survey, Value Added Tax (VAT), the predominant taxation method across the European Union, is a multi-billion euro fraud issue in its own right.



Source: CFCA Global Fraud Loss Survey 2015

Premium number fraud

For many fraudsters, the premium rate numbers assigned to “information services”, which generally offer a revenue share with the owners of the content, were a godsend. These were initially provided domestically (as “900” numbers in the US, for example) and then internationally, as specific ranges of numbers in expensive destinations such as Sao Tome and Principe. Such services used the very high international settlement rates to those countries to support the payments to the content providers.

As termination rates fell, and retail service providers started to monitor traffic (or even block traffic) to these esoteric destinations, some mobile operators in various countries assigned number ranges with a high termination rate to information services.

These premium rate numbers are a perfect way to extract money from the system and, coincidentally, to move money in a transparent and anonymous fashion from country to country, if that is the intent.

‘Premium number fraud is expected to reach US$16.8 billion in 2015’

In order to take advantage of premium numbers for fraudulent purposes, all the fraudster needs to do is to place some interesting audio content on the assigned number and market the service. Alternately, as many of them do, find a way to get traffic generated without the expense of marketing by paying someone to hack into a PBX and generate the calls without any intent to pay.

While the retail operator has to face numerous customer disputes and un-collectible invoices due to fraud, the wholesale carriers pass the traffic through the termination chain, paying each other for traffic terminated rapidly and with no fuss, and the final service provider at the far end pays the content owner. All very secure and anonymous, and the involvement of multiple international companies means that the fraud itself may have been committed in one country, but the true criminal is located somewhere else in the world. This means that law enforcement agencies are rarely interested in the complexities of an international crime such as this.

Don’t want to share the revenue with a distant mobile operator – perhaps an unallocated number fraud is what you need? Here the fraudster chooses some unassigned numbers in a reasonably expensive destination country (which are obviously never called by real people) and pumps traffic to these numbers. All they need to do is to get into the routing plan of a wholesaler and “terminate” these calls onto recordings. In return, they will be paid the normal termination rate for the country without ever having to provide a real service to that destination.

These basic methods can be seen in multiple variations of fraud involving retail service providers. What varies is the way that the calls are generated.

The key methods used include:

- PBX hacking
- Wangiri call generation
- Roaming call generation

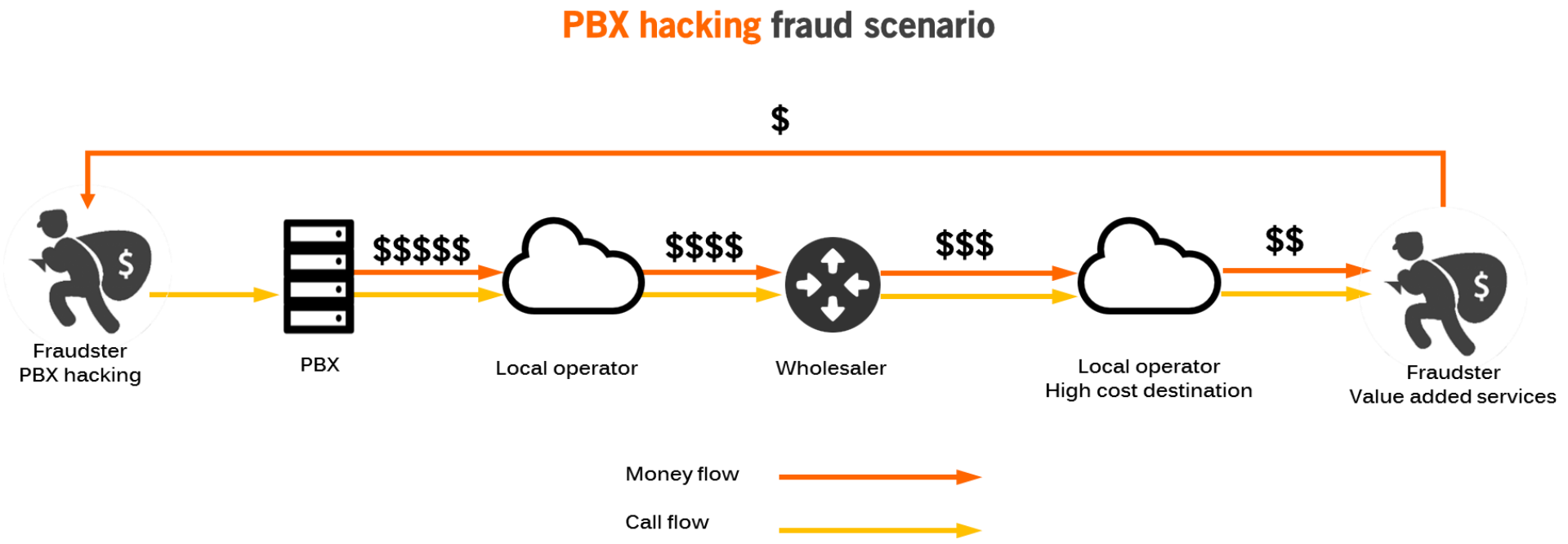
PBX hacking

Modern PBXs are much less secure, if poorly administered, than the old traditional exchanges. They are IP based and are connected to the public internet, so that employees can use them remotely. They are based in some cases on open source software such as Asterisk, and the admin addresses are often well known. If the password is weak, the hacker is in.

Once in control of the PBX, they can first test that the distant premium rate number is available and accessible with a few test calls. Then on a Friday evening, they can start to establish multiple calls to that expensive number, keeping them to a reasonable length to avoid simple threshold fraud management systems (FMS). They can play some music to avoid checks on the audio path for the call, and keep the system running until eventually traffic increases are detected and the PBX owner is warned.

Some more enterprising hackers prefer a slow and steady approach by sending a lower level of calls to the destination, but keeping it going 24 hours a day for a month or more until the invoice arrives and the company realizes, from the bill, what has been happening. A “below the radar” approach often generates more revenue than a “hit and run” approach and is more difficult to spot by simplistic FMS systems.

The PBX hacking approach is tried and tested, but in this case, someone needs to hack the PBX and some of the profits are shared with that person.



Source: HOT TELECOM

Wangiri call generation

Another approach that provides even more separation between criminal and call generation is the Wangiri fraud. In this method, the fraudster sends hundreds of thousands of call attempts to mobile customer numbers in a country. All of them are dropped after one ring leaving a missed call alert with a caller ID of the distant premium rate number. A certain percentage of customers are willing to call back the number to see who it was that called and are connected to a long involved recording aimed at keeping them online with perhaps news of a major prize they have won.

During that time, they are paying US$1 a minute or more for the privilege of listening to the message. When they finally get their bill, they of course dispute the charge, and in many cases, the mobile operator credits the cost of the call and supports the loss. The same approach can also use SMS or text messages to thousands of customers, again providing a callback number or an expensive premium text number.

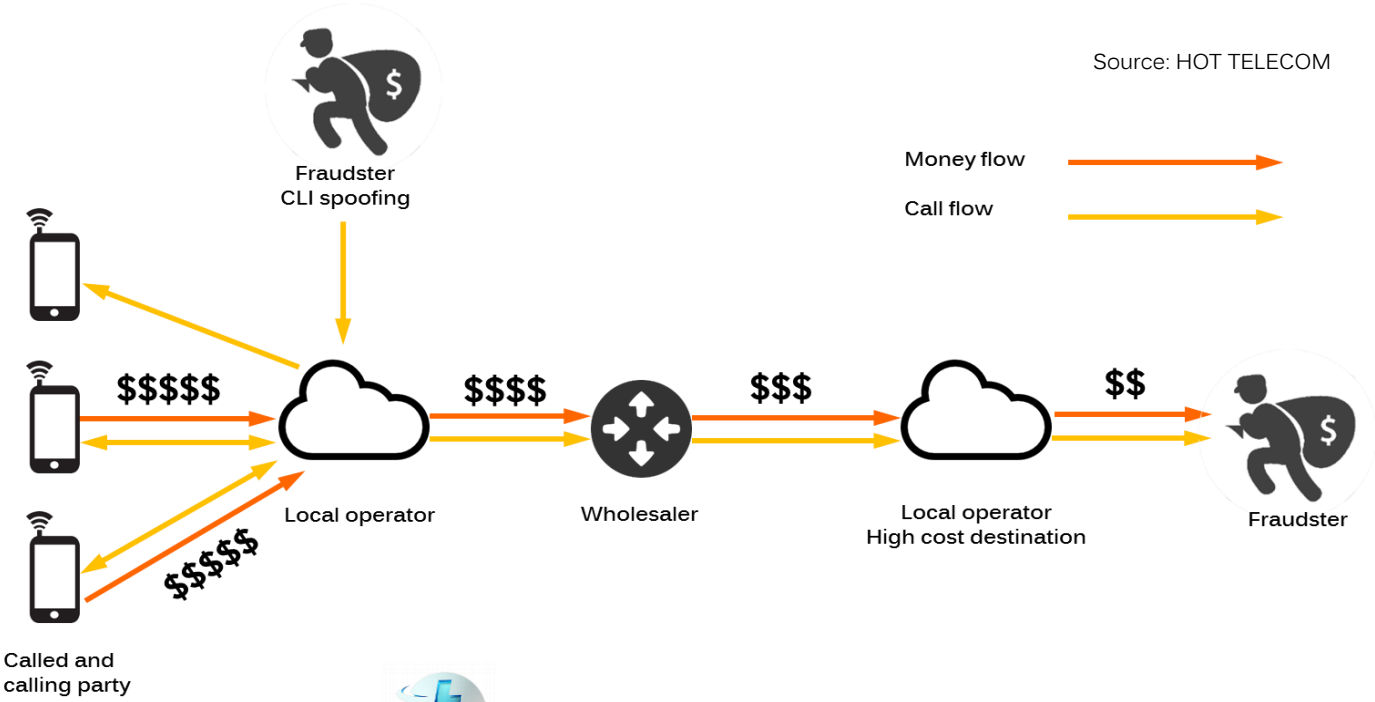
If the fraudster can gain access to an Application to Person (A2P) SMS grey route which bypasses normal billing mechanisms, all these initial texts can be generated at no cost.

Roaming call generation

This call generation approach uses mobile SIMs that are authorized to roam (or are clones of such SIMs). In this case, a SIMbox is used in the roaming country to generate multiple parallel calls via the roaming network to the premium number.This fraud works because of the relatively slow update of charges being incurred by roaming customers back in the home network systems. In the “old days” this could take several days, but even with more modern and speedy transfer of data, there is ample opportunity to make many calls before the SIM is disabled and the fraud stopped. Here the visited country will expect payment from the home network for calls made to these expensive destinations.

Wangiri fraud scenario

Source: HOT TELECOM



False Answer Supervision

Almost in a class of its own, False Answer Supervision (FAS) is a type of fraud that directly impact thousands of end users, but at such relatively low levels, that they rarely recognize it.

The basic approach is for one carrier in the chain of international wholesalers (often a mobile network because of the higher termination rates), to artificially extend the length of the call by charging for the ringing phase. This can add up to 30 to 40 seconds of billable time to each call, including charging for ringing for those calls that never actually get answered.

A variant, is for a carrier to route calls destined for UK mobiles, for example, to an announcement sounding like the person is just away from the phone and is coming back to pick up the call. Various domestic noises, including a barking dog, can add to the effect.

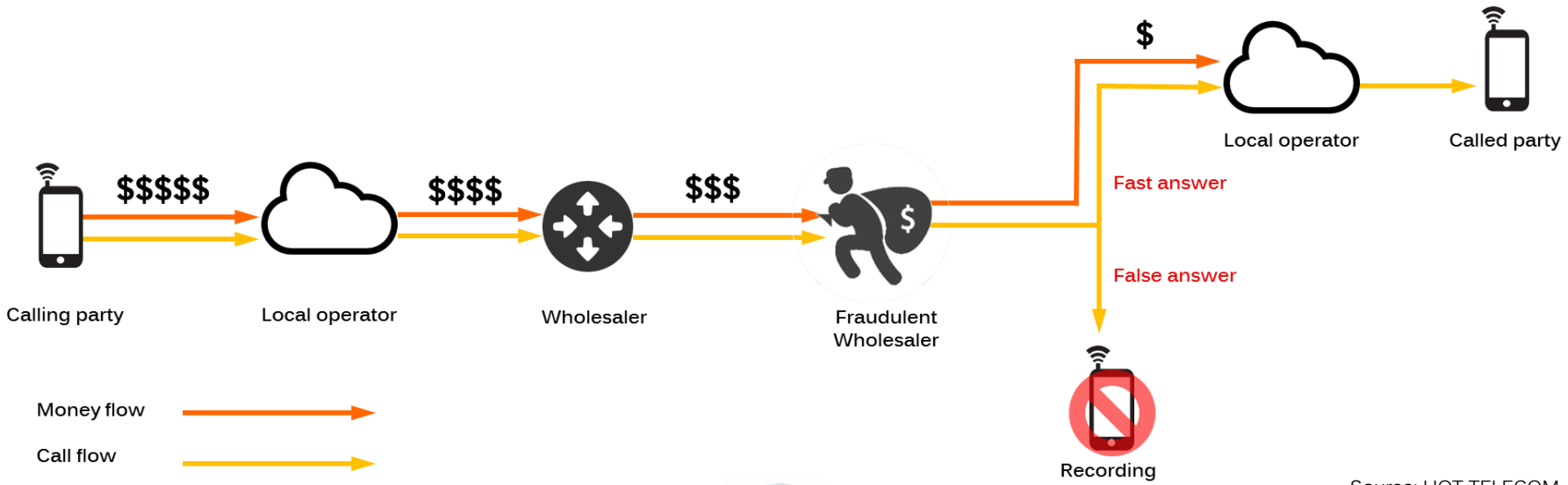
Without actually realizing it, the caller listens to this for a couple of minutes or more before finally thinking they have a wrong number.

Of course, they have been billed for the whole call, but rarely check their bill at that level.

Unfortunately for the industry, some smaller wholesalers see this fraud as a way of making a margin – being surprisingly open about their approach. They offer an unrealistically low price for a destination to get a lot of traffic and use FAS to make their margin. Their aim here is to do just enough to make a reasonable margin, but not so much that the fraud becomes obvious and they are removed from the route plan. This offering of an artificially low price then compounds the problem for legitimate wholesalers, as they now need to compete at this lower rate for the traffic.

FAS calls are far from evenly spread across destinations. While the fraud is underway, 20% to 40% of calls to a particular destination may be artificially extended, and then the activity will shift to another destination to avoid threshold based fraud detection mechanisms.

False Answer Supervision fraud scenarios



Source: HOT TELECOM

Commercial fraud

Each of the fraud mechanisms described so far impact end-users and their bill, and consequently their retail service providers, who often absorb the fraud to avoid losing the customer.

However, a more refined class of fraud looks for differences between the price of a commercial national service, that is perhaps legally available in a destination country, and the official international interconnect rate for that country.

Special pre-paid mobile offers are a case in point, where a local operator may offer a very low rate for on-net calls to customers on their mobile network. The underlying terms and conditions will seek to limit this to residential use, but enterprising groups will buy hundreds (or thousands) of the SIMs with this offer. They will then install them in SIMboxes that are specially designed to avoid detection and sell wholesale termination to that mobile operator via a VoIP connection to the SIMbox and an "over the air" connection to the called party.

Of course, the quality isn't great, the displayed caller ID is wrong, or marked as anonymous, and calls to ported numbers may not work. But generally, it is seen as "good enough" for some wholesalers to use the service and blend it in with more direct termination to lower their cost base.

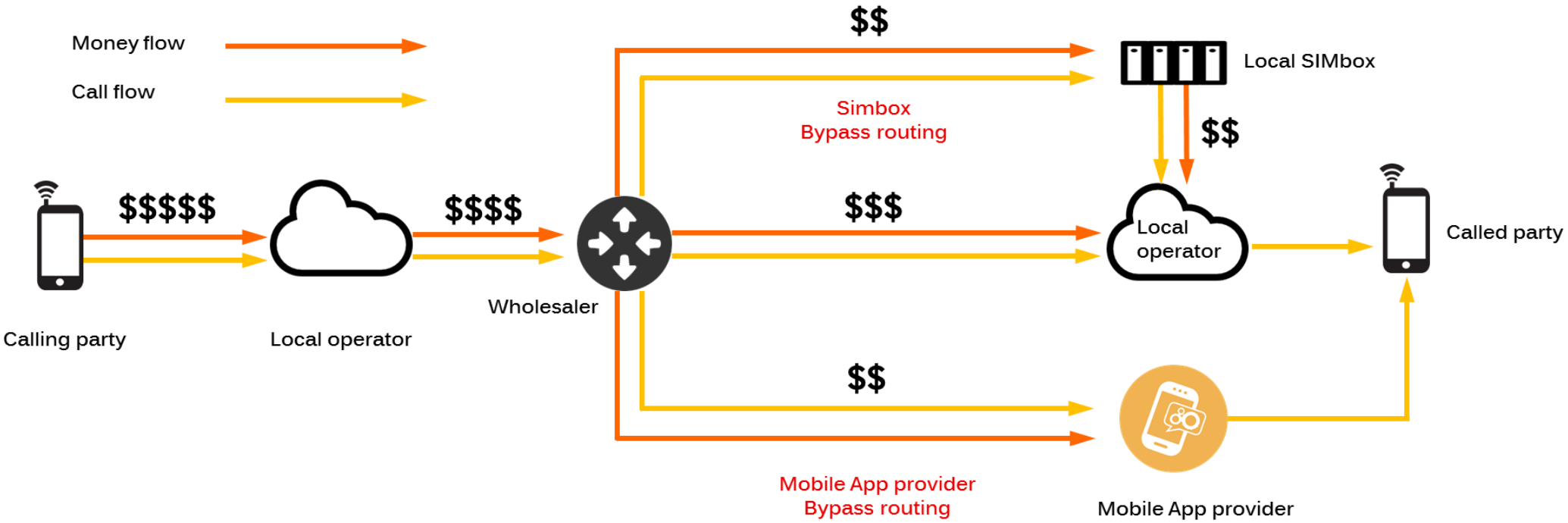
Unfortunately, for some smaller wholesalers, the concept of "providing a service" is alien. They are simply there to make money and their aim in trying to achieve "quality" is nothing more than providing just sufficient connections to maintain their position in the routing plans of other wholesalers. So if a call to a ported number is just dropped or routed to a local network announcement, that is OK, as long as their overall stats are maintained.

Mobile operator bypass

Some more recent developments of this concept involves Mobile App providers offering on-net conversations over the internet among other services. In this case, they can use the mobile telephone number of the handset as a user ID. To enhance their revenue, they have started offering a service that takes a normal telephone call to the handset and diverts it over the IP connection to the App client on the phone. The caller thinks they are calling the mobile telephone number of their contact, however the "call" ends up being answered by the App client of the called party.

Wholesalers who facilitate this scheme, benefit from a much reduced cost of termination offered by App providers, as this bypasses the regulated termination rate system. In return, customers experience an "OK" service, although it could be argued that the calling customer has been given something very different to what they thought they were paying for. In this case, the big losers are the destination mobile network (and the country through its tax receipts) who suffer from a significant reduction in revenue stream which would normally come from incoming call termination.

Commercial and Mobile App provider fraud scenario



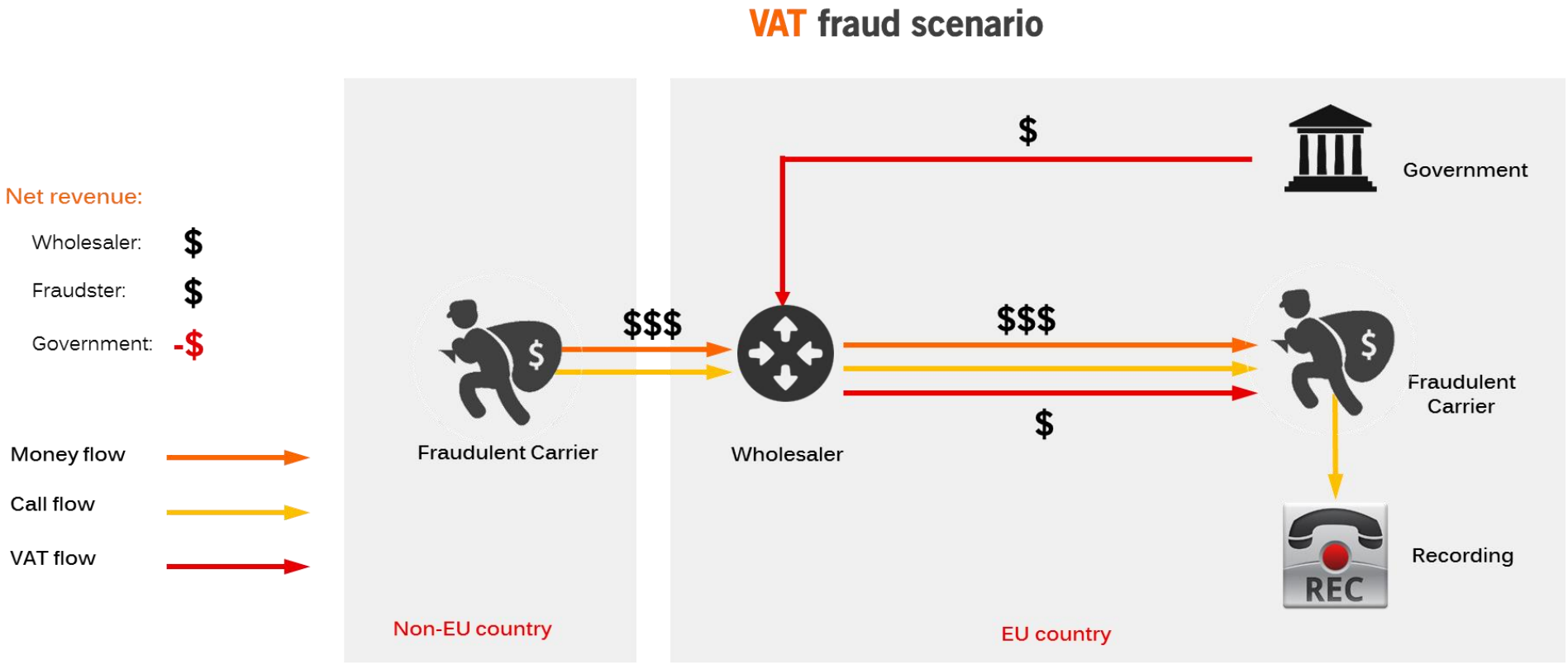
Source: HOT TELECOM

VAT fraud

As briefly mentioned earlier, Value added tax (VAT) fraud is itself a major problem with an increasing focus on the telecom industry. Some criminal gangs have established bogus carriers simply to make calls that originate in the US and are routed via a global wholesaler with operations in multiple countries to another bogus carrier based in Europe. The "calls" generally play recorded music to ensure that they are not dropped as a result of no audio being detected.

The charges for the traffic are paid, by the originating bogus carrier, to the global wholesaler in the US without VAT. They route it to their UK switch, for example, and connect it to the European bogus carrier, paying the cost of the call plus VAT (which can be 20% or more). However, they get to claim back that 20% tax from the tax authorities in the UK. Finally, the bogus European carrier fails to pay the VAT to the tax authorities and are able to make off with a 20% gain on the money they put into the scheme.

Through this approach, an instant 20% profit is made after accounting for the cost of the calls and, if the traffic is pumped to high levels, millions of dollars can be made in a relatively small period of time. The losers here are the tax authorities, although they are increasingly looking at the wholesaler to see if they should have known that something was amiss.



Source: HOT TELECOM

Why is fraud such a prolific business?

Perhaps the key reason that fraud is such a prolific business is that the profit motivation, quick returns and anonymity in telecom fraud, funds some very clever people to continually think up ways to avoid detection.

However, the attitude of some wholesalers, who profit from many of the frauds as well, has not helped. As we noted earlier, the defense that the call to Sao Tome was properly handled, rated and that the termination charges have already been paid, has been used for many years. The margin on such calls is high, the volumes when a fraud takes place can be equally high and wholesale is a cut-throat business....

Commercial frauds and False Answer Supervision are equally easy to ignore, often by claiming that; "It must be one of my suppliers that is doing that.... I'll open a trouble ticket with them..."

But, without a doubt, this attitude is changing – at least among the major wholesale carriers. This is partly driven by the realization that wholesale is evolving. There is increasing demand from mobile networks in particular for quality termination. In addition, the migration to IPX and to more direct routing will shrink the industry over the next few years. So the key focus for wholesalers is now shifting from being a supplier of low cost termination, towards becoming a long term, high quality partner.

In addition, the focus of the European tax collectors on the role of international wholesale businesses in VAT fraud is adding to this pressure. The prospect of jail time for not having systems in place to monitor un-natural telephone call flows will sharpen the mind of most telecom executives!

Fraud evolution

What do we see going forward? The continuing tightening of margins in wholesale voice means that a fraud to a destination that just costs a cent or two becomes worthwhile especially if the volumes are high.

That means that False Answer Supervision type cases will spread and become part of any destination over time. Premium rate frauds will continue to evolve, driven by the differing expectations of the players involved.

Mobile networks in developing countries, with their regulators, often need the income from incoming calls to premium numbers, and so it is unlikely that they will agree that such services are rarely used for legitimate purposes and clamp down on them.

What is likely to develop further are SMS driven frauds, where the SMS message is subject to a premium termination fee. As Application to Person (A2P) SMS takes off, it would seem to offer a perfect way to generate thousands of texts to a revenue share SMS service overseas.

'As fraud continues to evolve, smartphones will offer a new avenue to generate fraudulent calls and messages which are invisible to the customer'

A2P SMS and the grey routes that often are used, but loosely managed, gives further opportunities for fraudsters.

As smartphones become the de-facto "telephone" in many countries, the development of bogus Apps that purport to update a valid application, but instead include hidden code that generates calls or texts to expensive international destinations (and even are programmed to hide any warnings or alerts about account spending), have already been seen in use. As the growth of similar viruses for desktop machines have shown, we are probably at the tip of the iceberg with these types of Apps.

In the commercial fraud area, mobile operater bypass has highlighted what could be a growing tendency for a mobile operator to keep voice and messaging calls under their own control wherever their customer is in the world. With a WiFi connection automatically established, there is little need to make use of the visited network for any voice or messaging capability. That isn't fraud, as we have been defining it, but it certainly alters the way that international roaming and termination services can be handled and recompensed in future.

Also, it is perhaps too early to tell how VoLTE voice and video termination will be billed in the long term, but the complex signalling, especially when roaming, could open up ways to bill for services that were not completed as expected.

Moving outside the immediate environment of calls and texts, click fraud on internet based advertising is undoubtedly a big business. A wholesaler may not be directly able to address this, but it is worth bearing in mind.

The evolution from where we were a few years back, when fraud was known about but ignored at the wholesale level, to a situation now where some of the key carriers have very extensive fraud management platforms in place is a major progression. It gives hope that this increased visibility will identify frauds more rapidly and accurately as they evolve.

However, as we noted, the fraudsters are clever and often one step ahead of the carriers. So the million dollar question for most carriers is: 'What sort of systems and approaches are needed to be recognized as "leading edge" in this field?'

THE 7 LAYERS OF FRAUD MANAGEMENT

The winning strategy: An integrated approach

Most telecom professionals are aware of the Seven Layers of the Open Systems Interconnect (OSI) Model: from the physical layer of cables and satellite links, through networking components, to the application layer at the top. In practice, the entire telecom network can be defined in this way and it enables all the services we see around us.

To a large extent, the same approach needs to be taken with fraud management, as an holistic "soup to nuts" approach is the only way, in this day and age, to get ahead of the fraudsters. In other words, a simplistic threshold system, that alerts when traffic to Sao Tome (for example) rises above the normal level, will be prone to false alerts and will only incent the fraudster to restructure their approach to stay below the threshold.

Consequently, a carrier with such a simplistic system receives false alerts if the traffic naturally increases, but misses the true fraud that is just mingling among the normal calls to a specific country.

An added complexity is that fraud is not only a voice phenomenon anymore. In the same way that premium voice services were seen as nice revenue earners for mobile operators, premium SMS (text) destinations are equally attractive.

Few carriers have systems in place to monitor fraudulent SMS messages, so what better incentive is there to try this route to profit!

As a result, what is needed is an integrated fraud management approach that enable detection of activities to take place at all layers of the fraud environment, and for a multitude of services.

But what could these seven layers of fraud management be exactly?

7 Layers of Fraud management

Source: HOT TELECOM

7 Layers of fraud management

1. **Supplier validation and approval process**

   The key here is to have a solid process in place to validate that potential suppliers are likely to deliver fraud free performance, coupled with internal reports to block anyone from re-applying to be a supplier under a different company name if they have previously been removed.

2. **Comprehensive global routing plan**

   Routing plan generation and upkeep is a highly complex topic, as wholesalers generally want to sell to customers using a relatively simple plan, but then route traffic to suppliers making use of every possible breakout providing a commercial advantage.

   Having the ability to prevent fraud by automatically blocking call attempts to unallocated numbers (with the correct release that fails the call) significantly adds to the overall quality of service. Making use of services that offer authoritative and accurate global routing and numbering plans can be very cost effective in practice.

3. **Commercial validation of rate sheets**

   A new numbering range in a distant mobile network is often approved by their national regulator, but rarely publicized globally. The first indication of fraud may be the addition of a few codes to a more expensive destination in that country. As a result, comprehensive analytics flagging new expensive codes, especially for premium numbers, can directly feed into the fraud management system to flag potential fraudulent destinations.

4. **Advanced big data analytics**

   Nothing has changed in the world of fraud management as much as the statistical techniques now available to identify fraudulent calls.

   At a basic level, each individual call detail record or signalling message can look totally normal.

   However in aggregate, with complex statistical analysis, patterns of behaviour can be identified with a high degree of accuracy. Leading edge statistics (at the research level in many universities) can now be deployed to detect fraud with minimal false positives.

5. **Self learning statistical systems**

   Closely linked to big data, is the equally new concept of self learning systems. These do not require any threshold settings by “in-house experts”, as they learn what normal traffic behaviour looks like and they adjust, in real time, to changes as customer traffic ebbs and flows. In this way, the accuracy of a fraud alert increases substantially, which is key to the automation of fraud management.

6. **Integrated test calls**

   Some frauds, such as the use of SIMboxes for rate bypass, and particularly the newer mobile operator bypass approaches, are almost impossible to detect from the originating carrier records. In such cases, getting a direct confirmation of a fraud by sending a test call via the carrier in question is often helpful. As a result, integrating test call sending into the automated fraud management system can often be one of the aids to identifying and confirming these complex fraud types.

7. **Possible evolution to a networked solution**

   Carriers often share intelligence on frauds at industry conferences and more directly between the experts in each company. However, it generally requires a manual reaction. The potential for an OSS/BSS vendor with a widely deployed solution to automatically share approved information between systems can significantly improve the speed of detection.

An integrated approach

A key immediate issue is that no one fraud management system provider is equally good in all areas. For instance, Arptel has a powerful test call generation platform with global coverage, while IPsoft leads the field in automated, high accurate machine learning systems for False Answer Supervision and various premium rate frauds. TollShield, on the other hand, specializes in real-time detection and mitigation of international toll fraud. Implementing a full "7 layer" approach to fraud management can therefore put considerable strains on the internal IT organizations.

There is also another, often overlooked trait among carriers: the desire for home grown solutions to create a 'unique edge' on the competition. As fraud management has become so statistically based, there is a major danger with internal developments, where both specifiers and developers are limited by only "knowing what they know."

Engineers often have a reasonable level of statistical knowledge, but they are unaware of the latest machine learning approaches, for instance, and so their specifications usually rely on relatively basic statistical concepts. This is a significant downside if the intent is to automate the process from detection to remediation.

With such a focus on revenue and margin, a false alert that automatically removes a good supplier will result in all alerts being subject to manual validation, and from that point, the system fails due to the manpower demands it makes on the operations team.

As a result, perhaps the best approach is a mix of native OSS/BSS capabilities in business intelligence, analytics, and route optimization, fully integrated with the best of breed solutions in niche anti-fraud disciplines.

Alone among the global providers of OSS/BSS management systems, Telarix has taken this approach by enhancing its platforms to detect fraudulent, abusive, and arbitrage traffic, either natively or via a specialty anti-fraud partner, and providing integration with the carriers network to send out blocking requests, or to re-route traffic. Some of these capabilities include SIM-Box detection and triangulation, as well as identifying grey routes used to bypass wholesale international calls to local mobile operators.

Telarix could perhaps have developed all the components on their own, however they feel that creating an ecosystem with seamless integration with OSS/BSS provides the leading edge that carriers need to fight all aspects of telecom fraud.

Telarix's new anti-fraud module, iXDetect, works natively with the rest of its iXTools suite and integrates multiple components from leading practitioners of fraud management.

With access to an authoritative global numbering plan which identifies both unassigned and premium numbers, incoming supplier rate sheets, processed via iXLink, can immediately flag unassigned or new expensive code ranges for more detailed analysis or blocking on the network. iXDetect also has the capabilities to verify CLI delivery and mobile operator bypass via both integrated test call sending and statistical analysis of call detail records. Finally, it also supports FAS/premium rate detection using IPsoft and TollShield.

This integration of the best of breed in the fraud management ecosystem, into a single, easy to implement and operate fraud management system, has enabled Telarix to offer an all-encompassing solution. All this without requiring complex integration efforts from the IT teams of their carrier customers.

WHERE IS THE MONEY?

Does it make financial sense for wholesalers?

Of course, every business needs to make investment decisions based on sound and positive business cases. By its nature, fraud management is a potentially tricky case for wholesalers. The blocking of calls that are believed to be fraudulent to an expensive international premium rate destination actually decreases the revenue and margin that wholesaler would have earned if the calls had been allowed to proceed. So a simplistic business case focused purely on existing wholesale revenue has little chance of being positive.

Recognizing this, the i3Forum Fraud Group developed an ROI model for its members, initially to cover False Answer Supervision detection. Based on assumptions agreed by the membership, the ROI model calculated that a system detecting and removing FAS would result in a cash flow positive business case within six months. By rapidly removing FAS issues, the retail service providers no longer receive complaints from their end users and hence don't shift traffic to other providers. On top of this, the wholesaler gets more secure longer term traffic arrangements because the service is fraud free.

On premium rate frauds, wholesalers that are part of a mobile group (i.e. an entity that also has investments in mobile networks) can often pay for an FMS that detects these frauds with the revenue saved from just one or two incidents impacting their group mobile operators. Although they do not generally publicize the actual losses, it is well known in the industry that a loss of US$500K is not unusual in a single major incident. These are direct losses to the mobile group or retail service provider and hence reducing them provides an immediate financial benefit.

If the business case is extended to other retail service provider customers outside the group and the benefits of monitoring fraud on their behalf are included – which makes it far more difficult to migrate traffic away to other wholesalers – the case again turns positive in a matter of months.

Taken together as a '7 Layer' implementation, and benefiting from the integrated pricing that such approaches can provide, the case becomes more powerful.

At the end of the day though, fraud management is becoming a must have solution. Wholesalers are now operating in an environment where the majority of the traffic comes from mobile operators who are increasingly expecting very clean routing to support their high definition Voice over LTE traffic.

The carriers that are successful in this new high quality environment will not be the ones that cut corners to get another tenth of a cent off the cost. It will be those that are reliably trusted to maintain the best connection to the called party, while supporting all the features needed, with systems in place that immediately weed out any problematic suppliers. They will be the ones that help their retail service provider customers avoid frauds originating in their networks.

Pros & Cons of carrier fraud management

- ✓ **Traffic not removed because of fraud = more revenue**
- ✓ **Longer term relationship = more revenue**
- ✓ **Retail fraud stopped within Group = more revenue**
- ✓ **VAT fraud minimized = less jail time!**
- ✓ **Reputation as high quality = more revenue**
- ✓ **Fewer trouble tickets = lower cost**

- ✓ **Blocking fraudulent traffic = loss of revenue**

The first step towards greater carrier value

Although frauds often hit the end user and their retail service provider, wholesalers handling the traffic can no longer afford to hide behind their contract, as it demands payment for each properly connected call or message. Regulators are questioning this blinkered approach, tax authorities are concerned about the role of wholesalers in VAT fraud, and most importantly, retail service providers themselves are looking for help in managing this growing problem.

Forward looking wholesalers have already recognized that the opportunity is far greater than the short term loss of some profitable minutes. They have therefore invested in fraud management systems to add to the professionalism and quality of their offerings, and this is increasingly becoming a key differentiator in the marketplace. If, as we believe, the general trend will be to higher (and guaranteed) quality termination in the future, then extensive fraud management capabilities will be a key part of that offering.

Indeed, the fear of cyber-attacks, the damage that a widely spread bogus App infecting smartphones could do, and the general worries about privacy and security of on-line transactions makes this whole area one of key importance to wholesalers who are looking to expand beyond the simple termination of minutes. Having effective fraud management is the first step towards that goal.

Finally, developing a home grown fraud system is unlikely to meet that need. The complexity of the statistical systems able to detect frauds designed to fly under the radar, and to achieve this with no false positive alerts, can be overwhelming. In reality, most carriers do not have this expertise readily available in-house.

While individual fraud management vendors have their specialisms, it is also worth investigating solutions which offer the integration of best of breed offerings, with an ability to add incremental functionality towards the full '7 layer' implementation, as the market conditions require.

But at the end of the day, what makes a fraud management program successful?

1. **Integrated fraud management solution**

   A comprehensive fraud management solution will certainly address the '7 layers' we described earlier.

2. **Performance assurance**

   A key element is performance assurance: Does the vendor offer guarantees in terms of percentage of fraud detected and maximum level of false positive alerts? The ultimate goal is not to create alerts for fraud experts to analyze.

3. **Fraud management automation**

   The holy grail is to automate the process so that alerts feed directly back into network control systems to implement appropriate measures.

4. **Accuracy and reliability**

   Full automation requires all the elements above to work in an integrated fashion to provide both accuracy and reliability.

In our view, carriers should jump on the fraud management bandwagon now, and implement solutions that tackle this challenge, as this is not a problem that is going away anytime soon!

ABOUT US

The authors - HOT TELECOM

Isabelle Paradis, President, HOT TELECOM
Isabelle has the customer's experience at heart. She has spent the last 20 years working with over 100 Tier-1, Tier-2 operators and wholesalers on all continents, looking at how to improve and launch innovative services. She has written many reports, white papers and articles on the subject and has spent time looking at how telecom services are evolving, and what the future holds for the increasingly customer centric society.

Steve Heap, CTO, HOT TELECOM
Steve has a lifetime of experience in designing, engineering and operating networks, both domestic and international. With leadership experience in small technology start-ups through to global service providers, he has deep experience in a wide range of products, technologies and geographies. He has the rare skill of being able to explain complex technical issues in easily understood concepts and uses that extensively in his consulting work with Hot Telecom.

The sponsor - Telarix

Telarix, named the market leader in Interconnect Business Optimization solutions, helps solve a new set of challenges for international service providers with its software, iXTools® and iXLink®. The products, offered in both a licensed and SaaS version, are able to support voice, video, data and SMS.

Telarix also offers a managed service approach for carriers called Managed Interconnect Service. The service combines Telarix's award winning technology together with the technical expertise required to meet the specific business needs of your wholesale business. Staffed by subject matter experts with extensive knowledge and experience in routing optimization, interconnect management and revenue assurance, our MIS staff has an unique track record of enabling carriers to successfully optimize their key interconnect business functions.

HOT TELECOM

HOT TELECOM is one of the most innovative telecom research and consulting companies in the industry. With its head office in Montreal - Canada, HOT TELECOM's team is composed of International telecom experts based in America, Europe and Asia, giving it a unique insight into the global telecom market. It has served 200+ of the industry's leading operators, consulting firms and governments globally, providing them with Telecom Analysis and reports, Training and Consulting services across a wide range of subject areas.

For more information contact:

HOT TELECOM:
t: +1 514 270 1636
f: +1 215 701 7537
e: info@hottelecom.com
w: www.hottelecom.com

DISCLAIMER:

HOT TELECOM verified all information in this report to the best of its ability. The information contained herein has been obtained from sources believed to be reliable. However, as the information is based on a survey with mobile customers outside of our control, we cannot guarantee that the information provided is free of inaccuracies and/or fluctuations.

HOT TELECOM shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.