Revenue Assurance, Fraud & Security in 3G Telecom Services

Mark Johnson, VP Business Development

Visual Wireless AB

1. Background

New 3rd Generation (3G) services "have been built to create a strong attraction, almost addictive or viral in nature" (Nokia White Paper). 3G is a short term for third-generation wireless, and refers to near-future developments in personal and business wireless technology, especially mobile communications. This phase is expected to reach maturity between the years 2003 and 2005.

The third generation, as its name suggests, follows the first generation (1G) and second generation (2G) in wireless communications. The 1G period which began in the late 1970s, featured the first true mobile phone systems, known at first as "cellular mobile radio telephone." The 2G phase began in the 1990s, and much of this technology is still in use. The 2G phone features digital voice encoding, and examples include Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Global Standard for Mobile (GSM) Communications. Since its inception, 2G technologies have steadily improved, with increased bandwidth, packet routing, and the introduction of multimedia. The present state of mobile wireless communications is often called 2.5G, the best example being the Global Packet Radio System (GPRS).

Ultimately, 3G, which is being delivered primarily on the Universal Mobile Telecommunications System (UMTS) platform, is expected to include capabilities and features such as:

- Enhanced multimedia (voice, data, video, and remote control)
- Usability on all popular modes (cellular telephone, e-mail, paging, fax, videoconferencing, and Web browsing)
- Broad bandwidth and high speed (upwards of 2 Mbps)
- Routing flexibility (repeater, satellite, LAN)
- Operation at approximately 2 GHz transmit and receive frequencies
- Roaming capability throughout Europe, Japan, and North America

The ultimate 3G system will be operational from any location on, or over, the earth's surface, including use in homes, businesses, government offices, medical establishments, the military, personal and commercial land vehicles, private and commercial watercraft and marine craft, private and commercial aircraft (except where passenger use restrictions apply), portable (pedestrians, hikers, cyclists, campers), and space stations and spacecraft. [1]

The purpose of this Paper is to place on the table for discussion a short list of statements about our view of the 3G sector today, the nature of the threats to 3G operators from revenue leakage and fraud, and to society at large from the possible

[1] From Whatis?com

abuse of some features of the new services. We aim to start a dialogue within the industry about the steps we need to take collectively to avoid or mitigate these problems.

2. Market Analysis

The 3G telecom market is going through a trial by fire, its launch having coincided with the global collapse of telecom stocks and the drying up of investment. The delivery of enabling technology by infrastructure vendors is also delayed, as is network rollout. In some cases, operators have withdrawn their licence bids, and in others investors are increasingly nervous about the excessive size of many licence sales, particularly in the UK and Germany, where total 3G licence fees were over $50bn.

However, the success of I-mode in Japan combined with the overall demand for continuing technological enhancements and customer demand for specific services such as mobile broadband access, suggests strongly that 3G networks must eventually take off elsewhere.

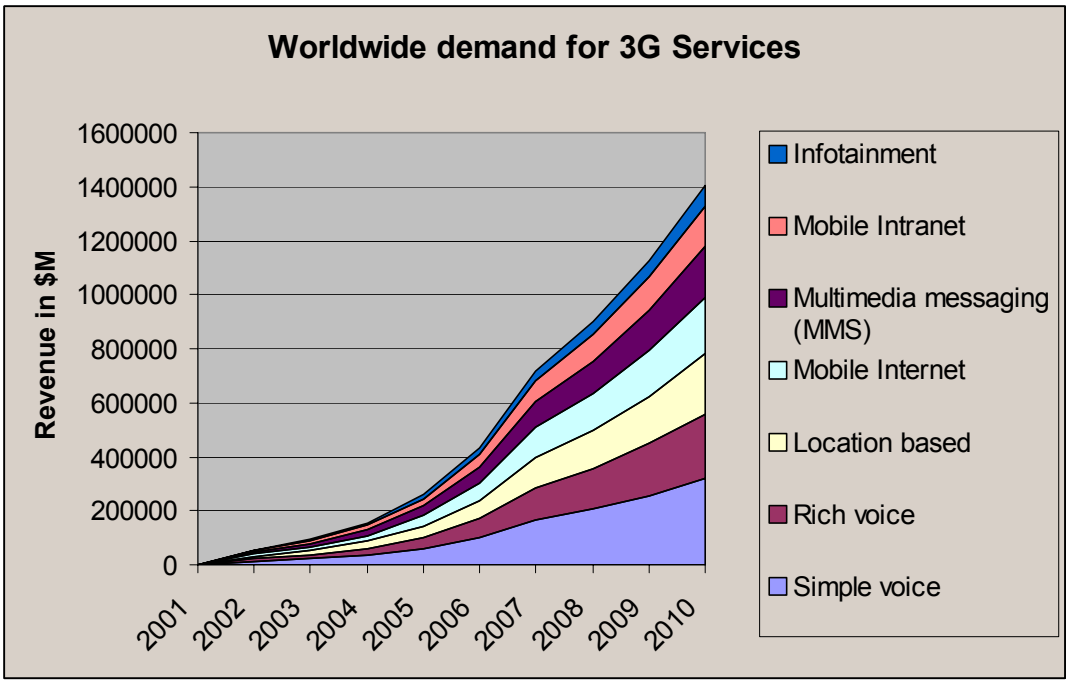
Much of the concern in the sector results from the expectation that UMTS would be the primary enabling technology for 3G. In spite of the delays experienced in Europe, there is evidence that delivery of 3G-type services will move ahead more rapidly in the USA, where alternatives to UMTS are being introduced. At the end of the day, it is the Next Generation ***business and services models*** that should concern us most, not the underlying technology.

3. Market Shape

Again, our only substantive evidence for the potential size of the 3G market is the Japanese experience. Many analysts have argued that we must be wary about drawing too many conclusions from I-mode's success, because Japanese culture is different from European culture. The Japanese often spend 3 or 4 hours per day commuting, for example, and therefore have much more time for M-commerce and infotainment.

However, the European experience with the Short Message Service (SMS), also called Text Messaging, which was originally seen as a minor feature to be offered free but which now accounts for 10% of GSM revenues, should teach us that we are more alike than we are different, and we should expect to see Next Generation networks in operation across most of Europe before the end of this decade. The smart money is still on the early delivery of a range of value-add services catering to the diverse needs of two key sectors:

- Business
- Youth



3G will not be able to compete with incumbent operators on simple voice services and the emphasis of 3G operators will therefore be on services that traditional operators find difficult or impossible to offer in a cost effective manner, for example:

- Broadband access
  - Video & audio streaming (infotainment)
  - File download (video, audio, still images)
  - Web browsing
- On-line services (e.g. banking)
- M-commerce (including micro payment transactions)
- E-mail and advanced picture messaging
- Location-based services
- Database access (e.g. Synchronised Corporate Calendar)
- Focused advertising

4. The 3G Competitive Landscape

In the early years a 3G operator's primary competition will not come from other 3G networks. It will come from incumbent 2G and 2.5G operators who will try to squeeze maximum benefit from their existing infrastructure in order to offer competing services. 2G operators are already offering a number of SMS-based services that are really lesser versions of some simple 3G services in disguise, and even GPRS, which has very limited service offerings at present, may one day get its act together.

This will confuse the picture for customers, most of whom will have little idea what 2G, 2.5G or 3G are, and in the short term this will probably be the source

of a great deal of pressure for new 3G operators. They will most likely respond by exploiting the more cost-effective infrastructure of UMTS and similar technologies to offer an increasingly wide range of products and services. These will be numbered in the hundreds from the outset, and in the thousands within a few years, with dozens of new services (many developed by third parties) being added daily.

This point is fundamental; a business model that shifts from a relatively static calling and rating plan towards a 'hypermarket' of constantly changing and evolving services, many of which will be designed to address very short-term business opportunities will change the way all suppliers of revenue assurance and fraud solutions are required to think about their products.

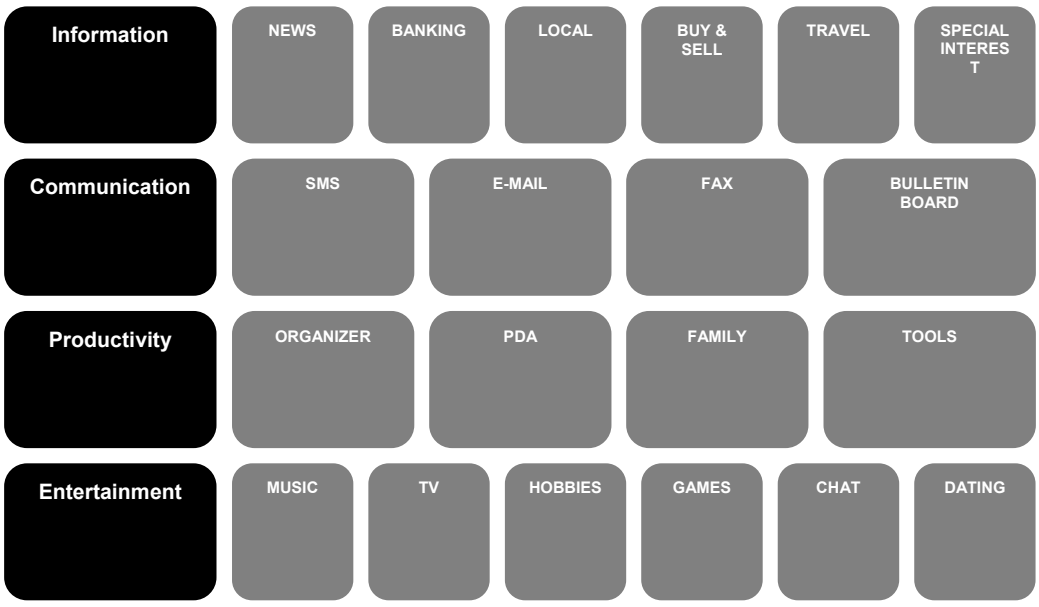
5. The 3G Business Model

As suggested, 3G operators will be forced to re-think the very meaning of 'telecommunications'. In fact, pure communication will probably be a relatively small slice of what the new operator is about. The operator will be positioned to address service and infotainment opportunities related to virtually every aspect of the customer's daily life, from food to travel, from sex to studies.

Operators are recognising this reality, and as a result there are three business concepts that are central to any discussion about the "3G future", as explained below.

5.1. The 3G Hypermarket of Services

Simply put, the concept of a hypermarket of 3G services refers to the point made previously; that operators will be positioned to address all aspects of the customer's lifestyle. The expectation is that, like a supermarket, the 3G operator will divide its offering onto segments, each focusing on a different aspect of life. Within these segments there will be foundation services (e-mail, web browsing,



Hypermarket of 3G Services as defined by Nokia.
Source: Nokia, Make Money with 3G Services White Paper.

etc.) 'seasonal specials' (e.g. cheaper picture messaging at Christmas) and 'one-off' services, such as ticket sales to next week's concert.

5.2. Towards a Market Segment of One

The second concept that operators are discussing is the theoretical market segment of one. This is the idea that, given enough data and enough computing power, it would one day be possible to address each individual customer as an individual human being with a unique lifestyle. So, for example, if Mark flies to London at 18:00 most Fridays, he could be offered information about airport traffic, the weather in London and films showing on Saturday and Sunday, all for a small fee. This information would be 'pushed' to Mark's phone, on the basis that if it is focused enough he will pay for it.

If advertising like this were to be pushed to a larger segment, a majority of recipients would probably be annoyed by the intrusion of such advertising on their handset, and extensive market segmentation and profiling is therefore seen as critical to the success of focused advertising, which in

turn is positioned as a service within 3G, and expected to account for significant revenues.

5.3. The Micro Payment

Traditional M-Commerce (the mobile form of E-Commerce or Internet commerce) requires a customer to logon to the Internet from a terminal and select items to purchase. In most cases, the customer is then required to input a credit card number to complete the purchase. The transaction therefore involves several parties and types of revenue transaction:

- A telecom network operator who supplies an access line.
- An Internet Service Provider (ISP) who supplies access from the telephone network to the Internet, typically for a monthly fee.
- The content provider who sells the actual items that the customer wants to purchase.
- The credit card issuer who supplies credit to the consumer.
- A clearinghouse may also be required to authorise certain transactions.

This is a complex model, with every player trying to capture a share of the customer's wallet, making M-Commerce more expensive than was originally expected, as well as being exposed to fraud. Anyone who is familiar with the 'dotcom' collapse appreciates how difficult it is to get a customer to take out his or her credit card and order on-line.

If 3G operators simply offer handsets that act as mobile Internet terminals, it is unlikely that M-commerce will offer the operator the kind of revenue opportunity needed to recoup the investments made. However, consider the fact that a major focus of the operator will be the youth market, where small purchases are the norm, as well as the fact that recent statistics indicate that 20% of purchases globally are for items worth under $14, and you have a major business opportunity for 3G operators, rather than a challenge, if the operator can develop an alternative business model. 3G operators have one distinct advantage in this scenario; the mobile terminal, with its SIM card, is both a device for browsing *and* a credit card. Purchases can be charged to the customer's telephone account, and all the customer has to do to accept the transaction is to press the 'Yes' button. Authentication and authorisation are carried out using the same processes already in place for voice calls, and by focusing on small transactions, the operator can reduce exposure to fraud and compete with the credit card companies.

This is the concept of the '**micro payment'**; tiny payments (expected to be typically 5c to 10c each) carried out in huge volumes by the collective customer base, and charged directly to the customer's 3G account with no middleman to take out the profits.

6. 3G Threats

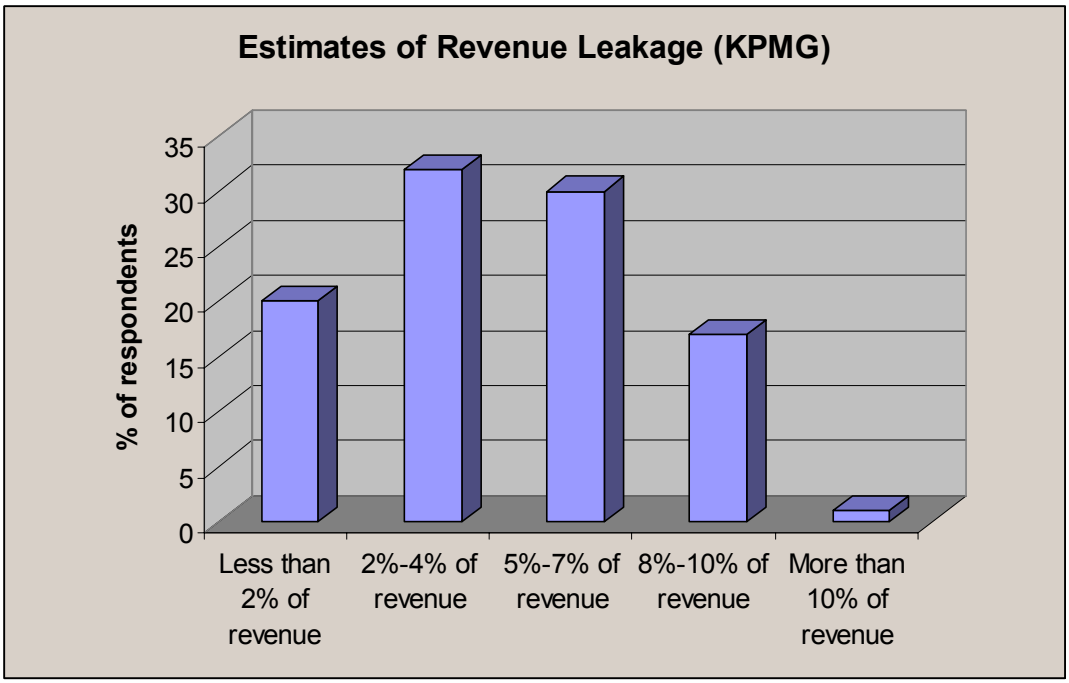
Up to this point, the challenge facing revenue assurance and fraud managers in telecom networks has been related to identifying unbilled and/or fraudulent traffic flows across their networks by analysing the data records created by network elements during call setup and handling.

Now the challenge is changing. Call data analysis does not address the unique features of 3G networks, and since revenue leakage and fraud are typically highest where the revenue focus is greatest, new approaches must be found to dealing with this task.

6.1. Revenue Assurance Issues in 3G

Even the most cursory examination of the 3G business model and resulting revenue flows, indicates that they will ultimately be far more complex than those for 2G networks. Notwithstanding our remarks about micro payments, 3G operators will also have to offer the traditional M-commerce model, as well as traditional voice, SMS and e-mail, plus all the new broadband and other services referred to earlier. Consider just this short list of revenue leakage points in 3G networks:

Location	Main Leakage Type
Switches	Data loss
CDR mediation	Data corruption
Voice call billing	Rating errors
Voice call settlement	Statement errors
Voice roaming	Data loss
Pre-paid calling & roaming	Fraud
SMS handling	Data loss
E-mail usage billing	Data loss
File transfer billing	QoS errors
Micro payment billing	Fraud
Micro payment settlement	Statement errors
M-commerce settlement	Statement errors
Micro payments while roaming	Fraud
Push advertising invoicing	Statement errors
Credit card settlements	Transaction repudiation
Clearing house charges	Statement errors
VAT collection & settlement	Over payment



Clearly, the Revenue Assurance function will need to re-tool and re-train in order to deal with this range of issues, and simply defining and enforcing financial liability between the various entities involved is likely to be a challenging task.

6.2. Fraud Issues in 3G

Fraud can also be expected to evolve in 3G. Today, the motive of the typical fraudster is to generate traffic to expensive destinations, such as international numbers or premium rate service lines. Calls may be of long duration or high volume, but the value of the fraud is a direct function of the volume of traffic.

Under 3G, this will change. In the context of broadband services, billing will be based on a combination of data volume and quality of service (e.g. bandwidth priorities, etc.). Where micro payments are employed, fraud will involve many small transactions that will be very difficult to distinguish from normal purchases. This means that much of the reasoning behind today's fraud management systems and processes will become redundant in 3G, and new thinking about solutions will be required.

Some of the typical fraud issues in the early 3G networks are expected to be:

6.2.1. Subscription fraud

This involves applications for service with faked ID or stolen and other documents, to get by credit checks and allow the use of telephone services with no intention to pay the ultimate bill.

6.2.2. Credit card fraud on M-Commerce

Purchases of goods and services on the Internet or from sites hosted by operators themselves will continue under 3G, and the credit card will remain as one payment option. Credit card fraud (card theft, forgery and transaction repudiation fraud) is very widespread in existing services and this pattern can be expected to repeat itself in 3G services.

6.2.3. Micro payment fraud

Possibly using subscription fraud as the primary technique, fraudsters can be expected to purchase goods using micro-payments, charged to their 3G-phone account, and then default on payment, possibly having re-sold those goods for cash.

6.2.4. Premium Rate Service (PRS) fraud

This is already a problem today, with some operators of PRS lines (e.g. sex lines) organising fraudulent calls to their own numbers in order to inflate incoming traffic and up their revenues. Under 3G, PRS will take new forms, with streaming video and audio, as well as still images being downloaded and viewed for a fee. Clearly, the same type of fraud as that which occurs today will be possible on these new services.

6.2.5. Copyright infringement and content resale frauds ('piracy')

As music and video become mainstream products within the 3G portfolio, we can expect sophisticated attacks on this media designed to support illegal copying and resale, in the same fashion as VCR and DVD pirating is carried out today. This will be an obvious draw for organised crime.

6.3 IP Security Issues in 3G

In addition to the issues already raised, we must remember that a 3G network is essentially an IP network. Because so many of the services on offer are basically Internet type services (e.g. E-mail, Browsing, Calendar Services, etc.) the 3G network and its handsets will be exposed to the full range of attacks that ISPs and consumers currently face on the Internet. Some examples are:

- **Hacking**; remote attacks typically intended to break or circumvent computer system or network security.
- **Denial of Service attacks**; attacks designed to halt service on a network or to a client of a network, for example by flooding a target node with e-mail traffic.
- **Viruses, Worms and Trojans**; self-replicating applications designed to copy themselves from one system to another (often in the form of

e-mail attachments) and to subsequently damage or exploit the host systems en-mass.

- **Data interception**; activities intended to steal data in transmission, such as credit card details or unencrypted passwords.
- **Database attacks**; activities intended to gain access to databases with the intention of exposing, altering or destroying data files.
- **Spam**; mass circulation unsolicited communications (typically e-mails or SMS in today's networks) often in the form of advertising.
- **Social engineering**; manipulation of customers' trust to obtain confidential information or to commit various scams.

Telecom operators are not in the habit of regarding the handset as a personal computing device connected to a mobile network. This must surely change with 3G, as both the commercial opportunities and the security issues become clear. In fact, the exposure of the 3G operator to viruses and similar attacks is somewhat higher than that of its fixed counterparts, for the simple reason that storage and processing limitations within the handset mean that security features such as virus detection software have been omitted in favour of chargeable features.

Some of the attacks listed will appear as part of a fraud scheme (for example, a virus attack that is designed to generate traffic from target handsets to a premium service) and the fraud team will need to see what's happening on the IP network if they are to adequately protect the customer.

Actually, the organisations responsible for securing the network, the customer and the operator's revenues, are set to evolve in as dramatic a fashion as the new networks themselves. The separation of tasks that exists today (Fraud, Risk, Security, IT Security, Network Security, Revenue Assurance, Credit Control & Collections) is no longer a viable model when a single service can incorporate elements falling within the domain of several or even all of these groups, and attacks can be similarly multi-faceted.

Our expectation is that 3G network operators will tend towards a single functional area with responsibility for all these issues.

6.3. Other Security & Law Enforcement Issues in 3G

Even at this early stage in the development of future services, it is apparent that the new capabilities that will be made available to the general public, with only minimal credit vetting and proof of identity requirements, offer significant opportunities for exploitation by the criminal element and by terrorists. Here are a few simple examples of possible scenarios:

6.3.1. Multi Media Messaging & Terrorism

A terrorist commander in a remote mountain hideaway in the Middle East requires a coordinated attack on several targets in the USA by separate operational cells. Information gleaned during the first attack will determine the exact target for subsequent attacks, but time is the critical factor as the follow-up attacks must be conducted before homeland defence forces can execute their contingency plans.

For security reasons, communication between each cell is prohibited, and it is also suspected that e-mail and voice communication to the commander may be monitored. However, using 3G pre-paid mobile handsets, obtained with only minimal security checks (easily bypassed) and the multi-media messaging service, operatives can photograph their targets and mission results, add text and audio, and transmit the results to any compatible handset in the world in a few seconds.

Under 3G, secure, encrypted, high speed data communications will have been placed in the hands of every terrorist, current or potential, in the world.

6.3.2. 3G Pre-paid Services and Money Laundering

A drug dealer has collected substantial sums of cash from his dealings and wishes to lodge this in various onshore bank accounts without raising suspicion. He uses his team to take out a number of pre-paid subscriptions, using faked identities. He then has his team members buy large denomination pre-paid top-ups in large volume, and he credits each account with several thousand dollars.

Using these heavily topped-up handsets, the dealer now purchases large quantities of merchandise in this simplified scenario. He then retails this merchandise from local stores, which he has rented or purchased, and lodges the proceeds in the bank, as legitimate takings from commerce.

3G in conjunction with the pre-paid service concept and loopholes in subscriber vetting and identification, places a sophisticated financial device capable of extensive cross-border utilisation in the hands of anonymous organised criminals, again on a global basis.

6.3.3. Multi Media Messaging & Paedophilia

A paedophile ring operating in the North East has been very restricted in its activities since interception of e-mail and investigation of web sites by law enforcement became widespread. With the new pre-paid picture messaging services, not only can they resume their communication in an anonymous and secure fashion, but they can transmit and view images in real-time from any location without being situated in a fixed location such as a garage or basement.

This sudden freedom does not only regenerate activity by previous offenders who had been operating under greater cover; it also brings a wave of new offenders into the area, who had previously been deterred by publicity about successful law enforcement operations. The service also allows commission of the offence in new locations and makes detection more difficult; a teacher standing to one side could, for example, take and transmit images of children in a swimming lesson, using a cell phone sitting innocently on his belt.

7. Conclusion

Law enforcement and corporate security professionals today face the most significant evolutionary step in communications technology and services since the advent of the Internet and the World Wide Web. Indeed, the mobile

nature of these new services combined with their far more rapid penetration in many markets, will make them significantly more difficult to deal with.

The community must act now to ensure that market forces do not drive the delivery of services that are wide open to various forms of abuse. Operators must be made accountable for what they sell, and they must make adequate provision for interception and information retrieval. Indeed, it may be argued that if operators wish to act as banks, then they must in turn be subject to the same rules and regulations as those that currently govern banking operations.

The most effective response of the law enforcement community, and of security professionals, will be to focus on regulation and compliance as the key mechanisms for controlling what is delivered to the general public. This will need to be a concerted and coordinated international effort, supported by legislators and, hopefully, by the 3G operators themselves.

About the Author

Mark Johnson (mark.johnson@visualwireless.com) is Vice President Business Development at Visual Wireless, a Swedish IT firm specializing in telecom revenue assurance and fraud management solutions. Visual Wireless is a leading supplier of Revenue Assurance solutions for fixed and wireless operators around the world. The tools and methodology are used to maximize the existing revenue streams, by minimizing fraud and operational leakage (www.visualwireless.com).

Mark entered the Telecom field in 1990, joining Cable & Wireless as their fraud manager for Latin America and Eastern Europe, working out of the company's London office. He was responsible for designing C&W's first automated fraud detection software application, and he subsequently went on to design similar tools for Alcatel, Ericsson and Nortel.

Mark started his professional career as an officer in HM Commonwealth military forces, serving in India and then in the Caribbean where he was operational in support of DEA in-country operations in Jamaica.

In the late 1980s Mark worked on special projects at the Port of Kingston, Jamaica, helping shipping lines such as Sea-Land and ZIM America to implement 'due diligence' procedures to prevent narcotics trafficking in containerised cargo, in line with US Customs requirements.