This article was first published in edited form
in Product & Image Security Magazine

Volume 14 No. 2 (March April 2010)
&
Volume 14 No. 3 (May June 2010)

# Airtime Reload Card Security

## 'Scratching the Surface'

March 26th 2010
(updated as White Paper
December 14th 2010)

By Nigel Page AMIEx

The Author can be contacted at:

nigel.page@sky.com
Tel: +44 7778 771 848

**Product & Image Security Foundation**

*Passionate about Product Protection*
**www.productandimagesecurity.org**

## Preview

In researching this article, I went right back to The Dawn of Time as far as mobile communications technology is concerned. In order to assess where the industry is now in terms of this article, it is important to understand where it came from.

Britain's first mobile phone call was made across the Vodafone network on 1st January 1985 by veteran comedian Ernie Wise.

However, the first ever call over a portable phone was made in 1973 in New York but it took 10 years for the first commercial mobile service to be launched.

The first fully commercial cellular network, known as the 1G generation, was launched by Japan's NTT in 1979. This covered the full metropolitan area of Tokyo's 20+ million residents, although within 5 years the network had rolled out across the country and had advanced into the 2G arena.

Denmark, Finland, Norway and Sweden followed in 1981 with the simultaneous launch of the 1G Nordic Mobile Telephone system. NMT was also the first network to introduce mobile roaming.

The UK was not far behind the rest of the world in setting up networks in 1985 that let people make calls while they walked.

The first call was made from St Katherine's Dock in East London to Vodafone's head office in Newbury, which at the time was over a curry house in the town centre!

For the first nine days of 1985 Vodafone was the only firm with a mobile network in the UK. Then, on 10th January Cellnet (now O2) launched its service.

Early model phones cost about £2,000, had a battery life of little more than 20 minutes and if not fixed into a vehicle, required a battery pack about the size of a briefcase. Car drivers fared little better. I vividly remember my first 'in car' company financed Motorola-branded phone requiring a battery pack of a similar size to be bracketed to the skeleton of the car's trunk, eating into valuable space normally reserved for product samples, brochures and other paraphernalia required on a daily basis.

Coverage was limited to main population centres, calls were expensive and the analogue radio signal technology was easy to eavesdrop on.

The first 2G digital cellular network technology was launched by Radiolinja in Finland in 1991 on the GSM standard, which also introduced competition in mobile telecoms when Radiolinja took on the 1G network operated by Telecom Finland.

The first data services emerged in 1993 with the advent of person-to-person SMS (short message service) text messaging in Finland. Additional data services such as payments systems, content services such as ringtones and full internet access followed by the end of the decade.

In the UK, Cellnet and Vodafone held a duopoly until 1993 when One2One (now T-Mobile) was launched. Orange launched its services in 1994. Both newcomers operated digital mobile networks from the outset.

In 2001, the first 3G network was deployed, again by NTT DoCoMo in Japan. This evolution promised enhanced data download speeds and arose via various step changes from 2G to the 2.5G General Packet Radio Services (GPRS) protocol, which offered WAP, MMS, Internet and email access, and onto 2.75G Enhanced Data rates for GSM Evolution (EDGE). This upgrade provides a potential three-fold increase in the capacity of GSM/GPRS networks.

Typically, 3G services available are mobile TV, video-conferencing, tele-medicine and location based services (weather, live traffic updates, vehicle tracking etc).

3G rollout remains ongoing across the globe, hampered in some countries by high additional spectrum licensing fees, and in many countries 3G networks do not work on the same radio frequencies as 2G networks, requiring the implementation of an entirely new network infrastructure in addition to licensing the new frequencies.

Fast forward to end of the first decade of the 21st century, and the industry is currently working towards the adoption of 4G services, specifically Long Term Evolution (LTE) and Ultra Mobile Broadband.

## Today

Mobile phones are omnipresent on every continent, in every country, in vast numbers. The world's largest individual network provider is China Mobile, with a staggering 500 million subscribers. The world's largest mobile operator group by subscribers is the UK based Vodafone. There are over 600 mobile operators and carriers operating commercially worldwide, and over 50 networks have in excess of 10 million customers, with a further 150 networks claiming in excess of 1 million subscribers each at the end of 2008.

Back in 1983 by comparison, Vodafone's business plan for the UK indicated that the network expected to achieve 2 million subscribers in total and Cellnet's expectations were for half that number. It took Vodafone 9 years to acquire the first million, but only 18 months more to double that number.

In Q308, just 5 handset manufacturers accounted for over 80% of all devices shipped worldwide.

From being the preserve of the wealthy, fortunate or corporate user in developed economies 25 to 30 years ago, mobile phone usage is now at the vanguard of communications for millions of ordinary people in the developing nations of the world, giving them a voice and access to commercial, educational, employment and social opportunities previously denied to their forefathers.

Wireless Intelligence (WI) reports that worldwide connections passed 5 billion by the middle of 2010, with over 1 billion new connections added in 18 months alone. Many markets have now reached saturation point, with over 100% penetration, or put more simply - more connections than population numbers. WI goes on to forecast in excess of 6 billion connections by midpoint in 2012. (For more information, see http://www.bbc.co.uk/news/10569081)

Much evidence exists that the technology has now reached the 'bottom of the economic pyramid' – an economic term to define the largest but poorest socio-economic group. In global terms, this refers to the 3 billion people who exist on less than $2.50 per day, and for whom the route out of poverty lies in new models of business that targets that demographic and through the use of new technologies.

I'm really talking about Africa here, as professionally I have spent much of my time over the past 5 years working in a number of key markets on this vast continent and witnessing at first hand the rapid pace of development.

Of course, these observations apply to many other parts of the world, particularly in SE Asia and the Indian sub-continent where the common denominators of massive population masses and huge land mass converging with antiquated fixed line, or in many cases, a lack of fixed line technology at all, have created this unquenchable thirst for this leading edge technology.

In Kenya for example, the population of around 39 million people was served by an out-dated, unreliable and expensive fixed network of around 300,000 lines for many years. These lines were confined to the major population centres, effectively cutting whole communities off from the outside world.

Today, there are now 4 operational mobile networks servicing approximately two thirds of the population and coverage is nationwide.

The recent and continuing huge success of mobile money transfer services operated by 2 of the networks – Safaricom & Zain (now Airtel) – as well as borderless roaming services operated by both networks in conjunction with sister or partner networks within the region and the wider continent provides further empirical evidence of the shift from hand out to hand up in these communities.

## Where is this leading?

For the networks to grow, to deploy the latest technology and to reduce the entry cost of access to services, they need to generate significant revenue streams from consumers. The Average Revenue Per User (ARPU) model is well documented elsewhere and generally rises in line with the availability and adoption of additional or new services by consumers. Effectively, customers are 'upsold' by the networks, although it is not uncommon for the average consumer of mobile services to employ multiple SIM cards from the range of networks to be used advantageously depending on the type or perhaps the time of day that the service is required.

This is possible because unlike in the UK for example, networks do not discount handsets or 'bundle' services in return for a fixed monthly charge. Limited banking infrastructures and informal cash based economic structures collude to ensure airtime sales revenue at the point of service delivery is vital. It is generally recognised that in excess of 95% of all connections in Africa are of a prepaid nature and airtime sales revenue from a variety of mechanisms drives the profitability of the networks and hence growth.

---

## Scratching the Surface

The mobile network airtime reload card, or scratch card to give it its more universal nomenclature, has been an instrumental part of the phenomenal growth of prepaid mobile telephony in the world's emerging economies over the past decade or so. While technological developments in prepaid systems have now annexed some of this space, the traditional scratch card still has a future. Although the format has evolved into multi-PIN ISO cards and low-cost strip vouchers, physical cards will continue to support the industry for some years to come. But how many of us know what is required to ensure this value bearing document, 'currency' unique to an individual network, remains resilient to fraudulent activity? Various processes are deployed by card manufacturers, but how suitable are they for this application?

This publication (which was first published in **Product & Image Security**) takes a look at this fascinating subject and features comment and insight from industry experts, drawn typically from the following disciplines:

- Mobile network operators
- Scratch card manufacturers
- Raw materials suppliers
- Freight forwarding and supply chain professionals
- Forensic agencies

We asked:

- Which type of substrate provides the best solution? Cardboard, Black centred board, plastic etc?
- What is the impact of 'over-scratch'?
- Scratch off materials - latex, foils, and labels. Which offers the best security for the network and ease of use for the consumer?
- Cost versus performance – what are the main drivers for networks in this area?
- Why prepaid cards? Why not another medium?
- What size & format are they? Why?
- How are they printed & personalised? What production methods are employed?
- What security features do they carry? Why?
- Data transfer, application and integrity control – how are these achieved?
- Card packaging – which methods provide the best security against theft or card attack prior to final consumer use?

- Card imports – what are the freight implications of transporting high value documents? What can freight companies do to ensure secure transportation from point of manufacturer to the client's nominated destination?

- What are the main risks associated with using the cards? From a user perspective? From a provider perspective?

- What forensic testing takes place? Is this done internally or via external laboratories?

- What is the future for prepaid airtime reload cards?

To the casual observer, or the uninitiated, the scratch card is nothing more than a token to be purchased, consumed and discarded almost immediately; a conduit to something more, a gateway to a world of mobile services, but with a life cycle at the point of final purchase of no more than a few seconds. For millions of people, this simple product is the primary interface between consumer and service provider.

From the street vendors in their brightly painted booths in Nairobi, to the hustle and bustle of Abdul Aziz Street in Cairo; to the aromatic coffee bars of Istanbul and the souks of Doha, the scratch card can be found everywhere.

As with so many outwardly simple interfaces, there is much more to the scratch card than meets the eye and this article – 'Scratching the Surface' – sets out to explore these questions and discuss what lies beneath the public perception.

## An airtime reload card is currency in another form

While addressing other requirements such as Brand Identity and Marketing, the scratch card, this 'brand in the hand' is first and foremost a functional, value bearing...and revenue protecting document. It carries a unique data code beneath the scratch off panel that when activated by the user, reloads the consumer's mobile airtime wallet with the value of airtime purchased. In that sense, the scratch card is the network operator's unique 'currency' note of tender.

And like currency, the scratch card must not only deliver the airtime revenue at the point of final purchase, but must also protect the very same revenue from attack from those who would seek to de-fraud the issuing network of that revenue.

Consequently, on the one hand, network providers are faced with the fine balance of delivering cost effective recharge cards in vast quantities throughout various levels of the supply chain, while on the other, deploying extensive Revenue Assurance and Fraud Prevention techniques to prevent leakage.

To put this into perspective, one major network has approximate annual face value sales of its lowest physical card airtime value, excluding other denominations and other forms or recharge, of an estimated $40 million, and volumes are rising.

## Security – Where does it start and where does it end?

In many respects, this is a loop; from design to manufacture to distribution.

From the perspective of the consumer, the retail infrastructure is highly fragmented, as the card generally passes through a number of different filters before final use, and this is typically on a daily or possibly twice daily basis, such is the nature of the micro economy of mobile recharge.

The issuing network can of course only sell its airtime once, and this is normally through its own branded and staffed retail outlets, or in bulk at a discount to a relatively small number of 'super dealers'. Activated cards are despatched or collected from the network's warehousing facilities, either on a centralised or regionalised basis for either direct sale or onward movement through the supply chain of thousands of independent re-sellers, usually on a hand to mouth basis. By this I mean the cash generated from stock purchased and sold to the consumer in the morning by an informal dealer is recycled into the afternoon's inventory and so the cycle continues.


*Airtime reload cards are a currency in another form. They require just the same attention to security detail with regard to authentication, counterfeit and forgery protection as applies to banknotes*

Cards are sold everywhere; from network branded stores, newspaper stands, filling stations, restaurants & coffee shops, under network branded umbrellas on the street and by young men 'door stepping' stationary vehicles in traffic jams.

It is therefore vital that the consumer has full confidence in the product on offer, made even more important by the move away from the traditional single PIN ISO format card, securely wrapped in its own film pouch, to the now more common 'portion', already unwrapped and sold in the open.

From the network operator's perspective, it should take into careful consideration 'the where, the how and the who' when selecting the scope of its recharge card offer, insofar as format, place of production and which supplier or suppliers will be recruited to provide these services.

Today, there is a plethora of manufacturing supply options for a network to consider. The cost of entry into the market for a manufacturer is relatively incidental relative to the potential volumes available and payback on capital investment can be attractive.

Only around a decade ago, there were relatively few manufacturers capable of producing these products, and it was common for scratch cards to be produced outside the country of consumption, particularly where the developing world was concerned. Access to developed world manufacturing infrastructure and skills were highly sought after by the emerging networks, and of course these new mobile players provided much needed new revenue streams for the suppliers concerned as the scratch card was made progressively obsolete in their home markets through the advent of alternative electronic recharge mechanisms. There was also a perception, rightly or wrongly, that it was safer to have cards manufactured thousands of miles away to prevent collusion to defraud the network of its data by disaffected employees working in tandem with similarly disaffected employees of a local card supplier. It was a 'win win' situation.

Fast forward to today, and card manufacturing now takes place on a global scale.

Entrepreneurs will always enter growing markets to capitalise on the opportunities before them, and as the networks grow, so there is pressure to localise the supply chain and provide wealth creating opportunities and jobs for the local population. Additionally, the necessity to maximise profit and reduce cost has seen this move towards local or regional supply as networks remove the collective burdens of freight cost, import duties and higher production costs as the market matures and local vendors catch up. In essence, this is a reverse of globalisation seen elsewhere.

Some established manufacturers have formed alliances or joint ventures to retain market share, and there has been a rise of outsourcing specialists; companies that find, develop and maintain network customer relationships while not being burdened with the overhead costs of running factories. Instead, these companies work with carefully approved production partners, usually strategically located and configured to give the best 'reach' and product mix into a number of worldwide markets.

This diversity creates opportunities, but also potential concerns, for network operators when selecting suppliers, and has given rise to 'detail rich' RFQ procedures and requirements over recent years, particularly as networks have grown, become more sophisticated and in many cases, acquired by larger multi-national brand owners.

While it is possible to enter the market relatively easily, network operators usually require suppliers, wherever they may be located, to operate to certain internationally recognised standards. These normally include current ISO accreditations 9001, 27001 and, for the environmentally conscious, 14001. Increasingly, EMV accreditation is now required.

Production should take place in secure facilities, away from public access and ideally with one central point of entry to site. It is not uncommon for these sites to have secure gatehouse entry systems, guarding personnel and a pre-authorised visitor log. Staff backgrounds should be checked with the authorities prior to employment and only those members of staff with a genuine need to be in card production or data processing areas should be given access. All non-essential staff should be 'access denied' status. Visitors and external contractors should be accompanied at all times and mobile telephones and any other electronic devices carried should be quarantined while in the production environment. Movement of all staff and accompanied visitors around the building should be monitored via door entry (swipe cards, PIN code or biometric) and overt / covert camera surveillance systems. On the basis of 'layered security', the actual production area should be a highly secure zone in the central core of the building and all production should be carried out under additional camera surveillance.

Irrespective of format or shape, telecom scratch cards usually adhere to the following basics:

- Material – paperboard or plastic substrate
- Print – Lithographic or flexographic processes

- Data imposition – ink jet process from variable data file
- Scratch panel – silk screen, flexographic ink, hot stamp foil or label
- Wrapping & final packaging

## Card Design

Card design, while adhering to the client network's corporate identity policy, should take account of potential security issues in order to assist in minimising opportunities for fraudulent activity. It is not uncommon for networks to utilise either the in-house marketing department or to commission an external design agency for this purpose. While these designs meet the branding requirements, it is sometimes the case that specialist advice or consultancy would be better employed when reviewing the layout of particularly the reverse of the card. These designs often exclude any printed zone or 'confusion panel' onto which the unique data is positioned prior to covering with the scratch off material. This is particularly important when the substrate to be used in production does not include any of its own inherent security, such as a coloured centre. In many cases, artwork has to be modified by card manufacturers to 'retro fit' this feature, and in some cases this requirement has proved difficult to implement because of network resistance. One only has to look around the market to see the various initiatives employed by manufacturers to resolve this matter and as a result, for those of us 'in the trade' it has become easy in certain cases to identify precisely which manufacturer is responsible for supplying cards and who to.

Simon Collins, Technical Director of Praesidium Limited, a world leading UK based Business Assurance consultancy specialising in the telecoms industry, says "We specialise in security and quality testing of prepaid vouchers for manufacturers and telecom operators worldwide. Our service is aimed at providing manufacturers with a benchmark relating to the security and quality standards of their own product compared with those offered by other leading suppliers." Simon continues, "Our findings and results are based on a number of key security and quality related testing scenarios developed by Praesidium, and these include a review of the artwork, particularly with regard to the position of the panel on the reverse and the methods employed in the diffusion area to inhibit extraction of the number while the card appears to be untouched".

Because of the varying processes employed by manufacturers and the differing requirements of network operators, it is difficult to regulate a standard for all to adhere to in this area, but one thing is sure; design integrity and consultancy need to be at the top of the list when commissioning or amending card programmes.

## Which type of substrate provides the best solution?

We wanted to know what the market thought about substrates; which provided the best solutions. While we received contributions from a variety of sources, it is clear that this is a very important area for all sectors of the industry.

Overall, cardboard based substrates were deemed to be preferable and plastics, while still popular in certain markets, are slowly being replaced. This is for a number of reasons, chiefly environmental, with the impact of $CO^2$ emissions into the atmosphere and landfill constraints. Plastic cards may be more durable than cardboard, but given that the average life span of a card at the point of final use is only a few seconds, it does appear slightly excessive to use this type of material for what is after all a disposable product.


*Cardboard based substrates are seen as preferable to plastics for environmental reasons*

From a production cost perspective, plastics are usually more expensive to produce, and in certain cases the static contained in the material leads to difficulties when printing the base stock and therefore costly wastage. Plastic is also bulkier and heavier in many cases and this has a significant effect on transportation costs, particularly concerning air freight, where weight and cubic calculations come into play when assessing shipping costs.

Abdul Mia, the former GSM Africa Fraud Forum Chairman, and internationally respected Revenue Assurance & Fraud expert, who has worked with a number of networks in Africa and further afield said when talking to me last year that in his view "It is a case of operator responsibility when it comes to the plastic versus cardboard debate". Abdul went on to say, "In developing markets, it should always be cardboard and bio-degradable products. In Iran, we used cardboard as well, and I'm not sure why certain Middle Eastern countries still prefer plastic.

If it is an over-scratch issue, then there are better solutions, such as using varnishes on the panel that could be adopted".

On the subject of card denomination, or face value, Abdul's states, "It depends on the denomination of the cards. In my view, high value denominations need to be manufactured on black centred cardboard material, while low denomination cards should be OK on standard boards". He concluded. "In my view, plastic is a 'no no', especially from an environmental perspective".

Simon Collins from Praesidium broadly agrees with Abdul Mia's position in this area. He told 'Product & Image Security' that in his view, "The voucher substrate is only one element of security consideration as different substrates carry an element of risk which can result in the monetary value of the card being compromised. For example, while a black cored body provides extra light restricting properties and should in theory provide a robust solution, in reality the black cored body layer can in certain instances be separated from the other substrate layers exposing the data code line to attack from light sources. This risk is also inherent in standard cardboard or paper vouchers."

He continued, "While it is not possible to split plastic vouchers, they are less environmentally friendly and depending on the plastic composition and label type used, can be compromised when subjected to different tests".

Dr John Drinkwater, Managing Director of Holographic Security Innovations Ltd, a specialist UK based supplier of holographic and printed scratch off foil and scratch off labels for the Atlantic Zeiser phonecard manufacturing environment agrees with the general points raised by Simon & Abdul, telling 'Product & Image Security' that, "All 3 are in use in various regions. Plastic is still utilised, but less frequently these days. It is obviously durable and has good resistance to over-scratch, but there can be issues with number indent visible on the scratch panel". He continued, "Black core is the traditional variant, with numbering onto a firm, calendared paper and then with scratch foil or label applied. Standard cardboard is a lower cost option, but to maintain opacity very high opacity scratch foils have had to be developed".

Taking up Abdul's point of varnish or lacquer applied to the PIN panel itself, John told us, "Some cardboard cards can use lacquered panels, but again one has to look at the lacquer bond to the number, as this can rub off with the scratch panel. Finally, there is the issue of matching the scratch foil to the lacquer for foiling speed".

Martin Horn, Director of Cape Town's Securi-Tech SA (Pty) Ltd, offers this interesting viewpoint, telling me, "Certain types of paper board used together with inherently secure scratch panel technology provide the best solution since they are inexpensive, secure and biodegradable".

He continued, "Black centred board is not a good solution at all since it is vulnerable to attack by de-lamination and therefore provides only a false sense of security. The best cards always have scratch panels that are inherently secure against reading of the variable data by any methods, including show-through using bright lights or lasers. This makes the use of a black centred board completely redundant and only adds unnecessary extra cost. On the other hand, if the scratch panel is not inherently secure and the card relies on the use of black centred board as a necessary 'security' feature, then the card is actually not secure at all. A fraudster can delaminate it, read the PIN, and then stick the layers back together".

"Plastic is very expensive and, more importantly, not at all environmentally friendly in production, nor biodegradable after use. Being extremely durable, plastic cards also introduce a significant security risk to telecoms operators since fraudsters can easily re-apply scratch panels to used cards and "recycle" the cards back into the market as new ones".

## What is the impact of 'over-scratch'?

Predictably, this drew a significant response from our respondents when we posed this question, drawing a number of interesting views on both the causes and effects of this. Alongside deliberate fraud, over-scratch and the dialling out of this ever-present problem occupies all sections of the industry to one extent or another.

Securi-Tech's Martin Horn told me, "Over-scratch usually occurs when a consumer scratches the card against or with an object that is too abrasive. When that occurs, not only is the scratch panel removed, but the PIN code is also scratched off, making it unreadable or only partially readable and therefore unusable. The consumer then usually calls the network's call centre, or returns to the retailer to demand a new scratch card or to be topped up with the equivalent airtime".

He detailed a number of areas what the potential implications of an over-scratch issue are:

- A free call to the telecoms operator's help desk costs about US$1.00 to provide the service needed to sort out the consumer's problem
- The consumer's (and retailer's) confidence in the brand is damaged

- The consumer is at times badly inconvenienced
- The telecoms operator has paid for a physical card that does not work
- The telecoms operator potentially loses the calls that would have been made had the consumer had airtime

Martin continued, "It is worth noting that such over scratch is less common in cases where the printed PIN number is covered with an extra layer of clear material that physically separates it from the scratch panel material and thus protects the PIN during the scratching process. This is the primary reason why certain telecoms operators choose to use non-secure scratch labels - the transparent plastic base of the label sits on top of the PIN number and protects it from damage. Telecoms operators using these label scratch panels are either not aware of the above fraud risk, or in many cases, they have simply decided to accept this risk rather than suffer from over scratch problems with all of the accompanying problems and costs".

"Fortunately, such trade-offs between PIN security and PIN durability against over scratch are no longer necessary for telecoms operators to make. Here at Securi-Tech, we've recently developed a new secure TUFF Voucher Technology that makes the PIN number more durable and this renders over-scratch virtually impossible. This technology, combined with our fully secure scratch panels, provides totally secure cards with little or no risk of over scratch".

From Abdul Mia's perspective, involuntary destruction of the card body can occur through the use of inappropriate implements. "People use nails, pieces of metal and glass to get to the number, rather than coins or fingernails", he told us. "It is the use of these objects that causes the card to be destroyed", he continued.

"What we have done is to measure the number of such cases and then put in place systems to ensure that the subscribers get what is due to them without the network losing out due to fraud. An example of this would be to ensure these calls go through to a specific number of agents in the customer care centre who can access the full PIN code, although for the airtime to be uploaded, the customer must be able to give the agent some of the digits to validate that the customer is in possession of the damaged card, and hasn't just picked a discarded one from the street. This corroborates the customer's claim".

Simon Collins has a slightly different take on this subject. "Over-scratch is predominantly a quality issue and can be as a result of the scratch panel application process deployed by the card manufacturer. As a result, network operators have to manage the customer impact and complaints, as end users are often unable to use the voucher for recharging". He continued, "Customer service activity increases manpower requirements within the Customer Care department in order to handle the level of complaints. The other main issue is the loss of revenue for the operator if their policy is to replace the voucher at full value and having to manage this process internally".

Simon concluded that "In a number of instances we have witnessed a lack of quality checking within the production environment on a batch-by-batch or machine-by-machine basis which with effective QC procedures would have identified inherent quality issues relating to over-scratch".

Abdul Mia's opinion is slightly different again. He believes education of the customer is equally important, particularly as it is very difficult to legislate against this common problem. He told us, "Messages on the recharge card on how to reveal the PIN is a way to educate customers not to use methods that will destroy the card. I found that it wasn't cost-effective to implement significant specification changes for this type of issue, especially when the average time a person has a recharge card in their hands is less than 30 seconds".

He concludes, "Basically, I would say this is an education issue, meaning education of the subscriber via marketing, on card instructions and via the call centre when users call in with such problems".

When **'Product & Image Security'** posed this question to John Drinkwater, he told us, "Care has to be taken to ensure the foil when first applied is soft to scratch off; that it has long term stability and remains soft and easy to remove. This can be a tough issue if the end customer is planning to warehouse the cards for long periods of time, possibly 6 months or longer, in aggressive conditions, such as near 100% humidity and ambient temperatures of 30-40°C. We've developed some specific formulations to deal with these problems".


*Tullis Russell, the specialist papermaking and coating group based in Scotland and North Western England began their development of an opaque phone-card board in 2004*

Dr Drinkwater's view on over-scratch where labels are utilised was quite specific. He told us, "Scratch labels are better to avoid over-scratch, but suffer the prime disadvantage of allowing easier access to the number than foils as labels can invariably be removed with some application of heat".

From the perspective of a paper maker, the UK's Tullis Russell, the specialist papermaking and coating group based in Scotland and North Western England began their development of an opaque phonecard board in 2004 when the company was approached by BemroseBooth Limited, a leading security printer and supplier of recharge cards to a number of African networks, to improve the security of the phonecard substrate deployed in card manufacturing.

"We already had a black centred product in our portfolio, which proved to be a good starting point", says Frances Darbyshire, Marketing Manager for Tullis Russell Coaters. "It had the required opacity but wasn't sufficiently robust enough for the subjective 20p coin scratch test. As we specialise in developing bespoke coatings for security printers it wasn't long before we developed a much improved anti-scratch layer together with an objective scratch test and specification".

"Consistency is of paramount importance in the security market", Frances continued. "The brand owner and end user must have confidence in the reliability of the phonecard. Where we started out thinking that opacity and anti-tampering were the critical parameters, we soon realised that it was most important to ensure that the end user, having paid for his or her card, didn't lose the PIN code through over-enthusiastic scratching".

"Early on in the process, we showed BemroseBooth our patented scratch card assembly which comprises two opaque coated layers. The lower layer contains a dark pigment to give added opacity while the upper layer has to mask the dark layer and give fine print performance". Frances told us, "BemroseBooth preferred this assembly to the competitor's laminated black centred product as the coated black opaque layer cannot be scratched away to reveal the PIN code without destroying the PIN itself".

"In conclusion", Frances said, "combined with the new improved anti-scratch layer this gave birth to the **tru**security® Phonecard".

Tullis Russell Coaters Ltd. uses **tru**card from Tullis Russell Papermakers as the foundation of their **tru**security® Phonecard. This comes with FSC credentials making the **tru**security® Phonecard the eco- friendly option for high value phonecards. **Tru**card is also popular with printers wishing to add the opacity at the printing stage.

Tullis Russell Coaters advocate the layered approach to security – it is possible to add extra security in every layer in the product. No one security feature addresses all needs and by having a multiplicity of specialised features, added at every stage in the supply chain, the card manufacturer outwits the fraudulent user and protects the end user.

My own view is that 'over-scratch' is a problem that will persist for as long as scratch cards are deployed as a recharge mechanism. The art in dealing with it comes from a combination of all the contributions raised in this section, but from first-hand experience, and as Abdul Mia advocates, education of subscribers must be given a high priority to avoid the issue in the first place. All too often we see the effects of this lack of awareness in the market, with cards punched right through to destruction way beyond the point at which the panel, usually successfully, has been removed. Networks must also hold their hands up and be stronger with such destruction and not replace these cards without question. I also accept that manufacturers have QC issues, particularly as John Drinkwater says, where aggressive conditions change the properties of the cards over time. But manufacturers must develop laboratory based plans to include ovens, abrasion testing, optimum scratch pressure and other methodologies and then build these into their specifications to be agreed with their clients to avoid damaging and costly claims for the manufacturer and brand damage to the network.

## Scratch off materials - latex, foils, and labels. Which offers the best security for the network and ease of use for the consumer?

As one would expect, opinions differ in the marketplace about what constitutes the 'best' solution. In some respects, the use of one scratch off solution versus another is driven by the manufacturing routes deployed by various suppliers. For example, ISO format cards personalised in sheet format are generally protected via silk screen printed panels with an overprint feature, usually bleeding over the edge of the scratch area for additional security. These cards are then guillotined and punched to final size before wrapping and packaging for despatch.

Cards that are personalised individually utilising the well established 'blank card in at one end, finished card out at the other' Atlantic Zeiser type route usually feature either foil or labels due to the production process.

Additionally, cards of other shapes and sizes can feature any or all of these processes, again depending on how the manufacturer is configured.

Abdul Mia told this magazine he favours foil with a logo, particularly when teamed with a black centred card body material and that labels do not sit flush with the card body, thus causing some aesthetic issues.

Simon Collins from Praesidium told us, “From a security perspective, hot stamp foil and silk screen latex type panels are typically more secure, because in most cases the ability to ‘lift & replace’ without showing visible damage is harder to achieve than with labels. However, hot stamp foil and latex type materials can result in more incidences of over-scratch if the material quality or application processes are inferior”.

Simon continued, “We’re reluctant to endorse the use of labels as in nearly all incidences the PIN code can be compromised with minimal effort. Even the more secure types of label products with enhanced degrees of designed-in security can be compromised by using various intrusion techniques”.

However, Simon also conceded that “From a customer experience perspective, label type products in our experience result in less quality or customer experience issues on over-scratching due to the design of the label. Praesidium has also witnessed a move by some operators to re-introduce less secure label type products to address over-scratch issues as the drive for customer satisfaction is viewed as being more important than security protection and reducing the risk of voucher compromise”.

John Drinkwater of Holographic Security Innovations offers this contribution to the debate - “In terms of our viewpoint, we manufacture mainly scratch off foil, holographic and printed, mainly for international phone card plants running Atlantic Zeiser ‘Cardline’ type machinery. We also produce scratch labels for the same customer base”.

“So, our scratch-off products are components of the card, but usually, and certainly in the case of holographic foil, this provides virtually all the security on the card and number protection against tape lift, show through etc. We therefore employ abnormally high levels of opacity in our products”.

“Our product needs to be applied at high speed, typically 25-30,000 cards per hour, virtually perfect to satisfy the intensive quality demands of the market, and needs to be removed very easily without number damage at the point of use. No easy task”.

Martin Horn told me, “Securi-Tech employs proprietary secure scratch panel technology on certain products and uses high security foils on others. Accredited GSM security consultants have confirmed the wisdom of these choices, as do independent laboratory tests using high-tech equipment. We’re extremely proud of our 7-year track record of never having a PIN number lost through fraud by any client using our cards”.

“However, the generic answer to this question depends on the technology used, since many grades of foil are not secure for scratch card use and do not pass the extensive security tests required by Securi-Tech SA and its clients. The same problems often apply to latex scratch panels, unless the manufacturer particularly adds extra features to improve the security”.

Martin has some robust views on the use of labels, opining, “Scratch panels in the form of a label applied on top of a printed PIN are, surprisingly, a fairly commonly used technology but in many cases this method is highly insecure, and we have hard evidence of why such scratch panels are not considered acceptable to Securi-Tech SA or any of its clients”.

The pictures on the following page illustrate this point very well, as they show the simple process of breaching a card protected with a scratch-off label. As Martin told this magazine, “The label was lifted easily in 10 seconds with a blade; the PIN was read and the label replaced undetected, allowing for resale by a fraudster”.


*Manufacturers of airtime reload cards often utilise specialist equipment such as the Edale Gamma press (above)*

From my experience, networks either adopt a laissez-faire approach to this very important area or specifically mandate for or against certain options. Anecdotal evidence against labels, for example, from one network was based on the 'lip' caused by the label sitting on top of the substrate, rather than flush with it (as in the case of silk screen or foil). Some of this network's users were trying to peel the label off, with the resultant destruction of the card. Sometimes, decisions are as marginal as that.

The bottom line is that whatever protection specified or accepted by networks must provide sufficient security to prevent random as well as sustained fraudulent activity as well as being easy to use or understand and prevent number destruction from the final consumer's perspective.


*Images show how insecure cards can be 'breached' with a sharp blade, the codes viewed and then the labels replaced*


*This process then provides the illusion of a 'new' card*


*A 'new' card created by successful blade attack*

## Cost versus performance – what are the main drivers for networks in this area?

There is fundamental agreement across the industry as a whole that cost is a prime driver for networks when operating physical card programmes. In many cases, production takes place externally to the country cards are consumed in, so factors such as freight charges, clearance fees and duties must be factored in. In one case I'm aware of imported cards can be as much as 37% more expensive when all factors are accounted for when compared to those procured locally. I haven't met one Supply Chain Manager yet who is happy to pay a significant premium for scratch cards as the product has become commoditised over the years.

Martin Horn again, "The answer to this question certainly depends on who is ultimately in charge of the card purchasing process at the telecoms operator. Purchase price is always an important consideration, but scratch cards are the 'life-blood' of many telecoms operators in pre-paid markets. The risks and financial consequences of poor performance can often far outweigh minor differences in purchase price. Multi-disciplinary purchasing teams aware of these risks need to consider what I call the 'Total Acquisition Cost' to the telecoms operator when buying recharge cards".

Martin then listed what this much broader calculation of total cost should include:

1. Costs of visiting supplier premises for quality and security audits:
    - Dependant on supplier location.
2. Delivered purchase price of cards.
3. Direct costs incurred by the network in performing incoming inspection, auditing, receiving cards into stock, data upload to billing system, picking for despatch and activation:
    - Dependant on the card supplier's accuracy of data files, the cards themselves, the packaging labels and the barcodes at each level of packaging.
4. Costs of holding stock, including warehousing and capital costs:
    - Stock quantities required are dependent on the service levels of the card supplier in terms of order to delivery lead-times, capacity flexibility and reliability of promised delivery dates.
5. Costs of missed deliveries. In extreme cases

telecoms operators have run out of card stock and so some try to protect themselves from this by means of punitive financial clauses in supply contracts. However, supplier penalties for each non-delivered scratch card valued at a few cents can never come close to compensating a telecoms operator for the lost revenue amounting to the several dollar face value of that same card which could have been sold to a consumer, nor for the loss of brand equity with both retailers and consumers when the telecoms operators cannot supply airtime. Indeed, SIM cards are so easy and cheap to obtain that the consumer in this situation can easily switch to a rival telecoms operator and this switch could become permanent.

6. Internal (national) re-distribution costs:

- Dependant on packaged weight and bulk of the chosen packaging specification.

7. Costs of poor quality and product or data security including:

- Poor product durability leading to over-scratched cards.
- Poor physical PIN security leading to compromised PINs & fraud in the marketplace.
- Poor data accuracy leading to duplicate cards.
- Missing or incomplete PIN under the scratch panel.

8. All of the above product quality and security issues can lead to:

- Call centre costs at approximately US$1.00 per call.
- Costs of product recalls and replacements
- Manual sorting of cards
- Deletion of PINs from billing platform
- New cards sent to distributors & retailers
- Distributor and retailer dissatisfaction
- Consumer inconvenience and dissatisfaction
- Lost sales opportunities in the field
- Loss of brand equity in the marketplace.

"Manufacturers remain under intense pressure to reduce costs" according to John Drinkwater. "However, performance still matters so in the end only products that work can be considered. Manufacturers must maintain quality while driving up output through higher running speeds and controlling their own costs in a better way", he continues.

Abdul Mia is in agreement, telling us that "More and more drivers are cost related. However, I don't believe that this is always the right decision and as I have already mentioned, the denomination value of the card should have some impact on cost reduction decisions".

John Drinkwater believes manufacturers must differentiate their offer and be innovative, but considers "Most of the big production plants are similarly equipped with card personalisation and wrapping lines, and this near standardisation makes it difficult to achieve this differentiation".

Suppliers find it difficult to leverage in many cases non cost related benefits such as accreditation, plant structure, R&D activity, reputation, customer service and other factors when price remains top of the list for networks. The dichotomy of high quality products that work at the point of use versus ever reducing prices is the eternal challenge for the industry.

As John Drinkwater concludes, "The basic scratch off parameters are generally the most important thing on the card, and quality issues here alone can and do lead to mass card rejections by networks".


*Airtime reload cards on sale in a typical African retail location*

## Why prepaid cards? Why not another medium?

Recent research has indicated that approximately one third of the entire world's population has a prepaid mobile account - some 2.45 billion customers. 43% of these customers are located in the Asia-Pacific region, and around 95% of all connections in Africa are prepaid. (Source: Global Mobile Prepaid Strategies & Forecasts to 2013, 8th Edition – Informa Telecoms & Media).

Indeed, the founder of the pan-African network 'Celtel' (rebranded as 'Zain' initially, and now rebranded again as 'Airtel'), Mo Ibrahim, is quoted as saying, "Mobile phones could not work in Africa without prepaid because it is a cash society". (Source: Economist Special Report, September 2009).

In 2007, overall worldwide revenues from prepaid accounts were in the region of $242 billion (Source: Global Mobile Prepaid Strategies & Forecasts to 2013, 8th Edition – Informa Telecoms & Media).

The simple truth is that there are many other recharge options available across the world. These include EVD (Electronic Voucher Distribution), SMS direct airtime transfer, ATM, lottery terminals, online Internet recharge, Direct Debit and other sources. However, despite the many available options, not all are appropriate to emerging markets for varying reasons and 15% of the overall volume of prepaid recharge in 2008 was attributed to the scratch card voucher. (Source: Global Mobile Prepaid Strategies & Forecasts to 2013, 8th Edition – Informa Telecoms & Media).

Securi-Tech's Martin Horn told 'Product & Image Security', "To maximise sales and avoid lost revenue opportunities, telecoms operators must ensure that airtime is readily available and convenient for consumers to purchase at all times on an as-needed basis. As many methods as possible are therefore used to achieve this and cater for all types of consumers".

"Thus, he continued, "the first key reason for prepaid cards is simply that they continue to fill many gaps in the distribution chains of telecoms operators that other methods cannot easily or practically reach. In developing countries, issues facing electronic and virtual recharge methods include the reliability of electricity supplies and the maintenance of technical equipment in remote areas with poor general infrastructure, as well as the ability of consumers to travel to formal retailers, and even their opening hours. By contrast, prepaid scratch cards have proved resilient and reliable in all environments as well as highly mobile, reaching consumers where they are and at any time of day".

"Secondly, many consumers have a variety of reasons to prefer prepaid cards as a recharge method. These reasons can be summarised as trust/peace of mind, postponing of use and speed of transaction".

"An unscratched card offers peace of mind to consumers wary of scams and fraud. With electronic methods offering virtual PINs, or PINs printed unprotected on unbranded slips of paper at or near the point of sale, consumers often cannot tell if the PIN has been used previously".

"Furthermore, consumers who live in remote areas often purchase airtime on their way to and from work in a city or town. They may not want to consume the airtime immediately, or might purchase it for a family member or friend or even for resale in an informal trading situation. Scratch cards provide a durable mechanism of postponing consumption and for facilitating resale".

"In developing countries, informal street vendors account for a large proportion of airtime sales. These people usually sell prepaid cards to passing consumers alongside snacks, drinks, cigarettes, etc. and the 'dwell time' involved in such street transactions is typically only a few seconds, especially during rush hour. In these situations neither street vendors nor consumers can really afford to wait for a virtual airtime transaction to be completed, as this can take anything from 30 seconds to several minutes. Both parties want something easy and fast and we've heard from our clients of many cases where, given the choice to sell the same airtime values at the same margins, virtual vendors have switched back immediately to using cards".

Martin concluded, "Prepaid cards provide a 'brand-in-hand' marketing opportunity for the telecoms operator during each recharge event. Increasingly, the trend is for prepaid consumers to recharge more often, usually with smaller airtime values. We think this presents a significant opportunity to build brand awareness with consumers as they 'touch' the brand every few days, but this opportunity is largely missed with electronic or virtual methods".

As Abdul Mia says "It depends on the market, but in Africa if you are paying for something it has to be tangible, like a card. Customers don't particularly like to receive a piece of paper with a visible number like a till receipt, or in other cases nothing at all". He went on to say that there is a tendency to move to other mediums as well, but believes it is a Marketing issue. "As people get comfortable with new methods they start using them more, and in South Africa in particular there is a move towards the virtual voucher".

John Drinkwater agrees. “Cards are used in vast quantities in emerging markets where a lack of a converged communications and banking infrastructure inhibits contracts, and they are sustained as a reliable method by reduced pricing levels to networks brought about by competition amongst suppliers and changing formats”.

Jannie Bester, Managing Director of Pro Scripto Document Examination CC based in Pretoria told me, “A recharge voucher is probably the most effective visual communication tool a network has to strengthen brand name awareness. Once purchased, it doesn’t need electricity and is immune to viruses and electronic sabotage. When something goes wrong with the voucher, hard evidence is available and reaction time to rectify is usually much shorter”.

Brand name awareness is vital to networks, as Jannie says. The available space for network operators is ever more congested with new entrants to market and the establishment of pan-continental operators. Independent networks jockey for market share alongside the international brands that have established operations locally or simply bought out rivals, and differentiation of offer is vital.

It is not uncommon to see subscribers switching SIM cards during the day to take advantage of differing tariff structures from rival operators, and networks are constantly developing retention or acquisition marketing strategies in the fight for market share.

One key area that the scratch card, perhaps uniquely, still has a role to play is in this promotional activity space. Cards can be used for game playing purposes such as ‘scratch & win’ initiatives, or they can be used to promote good causes, such as the environment, UNESCO etc.

Some years ago, Kenya’s Safaricom partnered with Strika Entertainment (Pty) Limited of Cape Town and the UK’s BemroseBooth to produce a limited edition run of cards carrying ‘Supa Strika’ and ‘Mighty Shabbs’ cartoon football players on the card face. Some 30 different images were produced to allow for 2 full teams and substitutes across 2 denomination values. The smaller number of higher profile ‘celebrity’ players were deliberately allocated to the higher denomination card and a promotional campaign was put in place to support the activity.

Football is incredibly popular across Africa, no more so than in Kenya and the exploits of the fictional ‘Supa Strika’ players had a huge following in Kenya through a dedicated website (resembling that of a real team), and a magazine inserted in one of the Sunday newspapers.

Card sales predictably rocketed as subscribers flocked to collect and trade cards between themselves to ensure all 30 were acquired. The promotion worked on many levels, but the real driver to the network was to prevent used cards being discarded in the street after use. Simple, but effective.

Jannie Bester concurs with our other experts’ views in that, “The balance between the need for physical recharge vouchers and virtual methods of top up are very much dictated by the client profile of the network and is also dependant on the country in which the network is doing business”.

Having spent a number of years at the sharp end of card sales to networks myself, my own view is that when given a choice the average prepaid customer in Africa, the taxi driver, the office worker, the hotel receptionist will always choose a physical product over any of the alternatives. It isn’t a scientific approach, but sometimes ‘vox pop’ is just as reliable. As noted earlier in this article, the sheer number of locations that cards are available from is staggering, providing actual evidence of the popularity of this medium.

We must not forget that prepaid card programmes also provide employment and wealth creating opportunities for those people who have joined the growing army of re-sellers far down the distribution network who position themselves at traffic interchanges, on street corners and in informal kiosks.


## What size & format are they? Why?

Scratch cards for this market have traditionally been to the ISO approved format and are the same size as banking cards. Generally speaking, this is because cards were originally produced on similar personalisation equipment to financial sector cards. There is also some informal evidence that this format had some perceived kudos as these single use, short life products resembled a more valuable and desirable product in the wallet.

Over the years, enterprising suppliers and networks have cooperated in the development of this format, and today we see the same ISO card body perforated into detachable sections, usually carrying between 2 and 5 individual recharge portions.

Networks had built their businesses on, relatively speaking, middle and higher income earners initially. These early adopters provided high levels of ARPU (Average Revenue Per User) to the networks and fuelled rapid growth and development of added value services. To capture additional consumers, networks needed to reach down to the bottom of the economic pyramid, to those consumers unable to get on air because of the high cost of airtime.

Thus, the 'multi-PIN ISO card' was born. Individual recharge denominations tumbled and subscriber rates went through the roof. In one case I'm aware of, annual consumption of individual vouchers rose from around 40 million cards per year to approximately 180 million, while the subscriber base tripled in the same period. This not only suggests more customers joined the network, but more of the existing customers elected to trade down and buy airtime as and when it was required, rather than purchasing in higher denomination amounts on a less frequent basis.

Abdul Mia again. "Cards are getting smaller, mainly due to the cost. In times where operators are squeezed more and more with margins, they are looking at other ways of making up for lost revenues and profits".

A few years ago, alternative formats started to appear on the market, normally in sheet or strip formats with a much smaller individual voucher profile. These vouchers are typically high volume, low denomination, low cost alternatives and bulk packed. After a period of resistance to change, more and more networks are starting to adopt these formats for at least part of their portfolio. In certain cases, networks have shifted their entire card offer away from the ISO format to clearly differentiate themselves from their rivals.

"Amongst our other innovations", Martin Horn told me, "Securi-Tech was the first company to create cost-effective cards for low denominations through our tear-off strip cards supplied in strings of 10. The other scratch card manufacturers realised the importance of our new cards but, because most did not have technology offering flexible formats, they launched credit card sized 2, 3, 4, and 5-part cards instead. However, Securi-Tech's 10-part strip cards retain the advantage since the packaged cards are lightweight and up to 10 times more compact to store and transport than conventional cards. From our research, we've calculated a 30% saving in redistribution costs over 4-part conventional cards".

He continued, "Strip cards are also more compact and fit easily in street vendors' pockets. This means that street vendors are able to carry more cards than they would with credit card sized cards. Each card can then be torn off easily during the sale to the end consumer".

"In developing countries, for telecoms operators that are already established, the trend is towards smaller cards, since consumers are now very familiar with using scratch cards and no longer need to be supplied with many detailed instructions printed on the card. Also, as the average value of a recharge transaction reduces, and the frequency of recharging increases, telecoms operators are looking to reduce cost per recharge card. Quite simply, the smaller card formats provide the means to do this".


*An airtime reload card is activated after sale*

## How are they printed & personalised? What production methods are employed?

It is possible to produce cards via varying processes and these are very much manufacturer specific.

Praesidium's Simon Collins told us, "From a voucher security perspective the manufacturing environment plays a pivotal role in providing end-to-end security management, but industry wide the position varies from vendor to vendor. Irrespective of the level of security incorporated into a voucher's technical specification and design, it is the level of security control and security protocols within the vendor that ultimately ensures an operator receives a secure product to the highest standards possible".

He continued, "If security related processes and controls are weak in any area of the manufacturing process including secure data management, printing and personalisation, this can result in a number of key security risks".

"For example, this could include the PIN codes being visible during the process and therefore potential for compromise. Defective vouchers that aren't correctly managed out of the process and the duplication of PIN codes are other areas of concern from a security perspective. In our view, there are a range of manufacturing failings could result in the operator experiencing security issues or even the manufacture of counterfeit vouchers".

"Furthermore", Simon told us, "Accepting that voucher PIN codes are unlikely to be active during the manufacturing process would not affect a fraudster's ability to quickly sell on inactive or discarded vouchers or PIN codes into the market place at a discounted price to unsuspecting customers. Fraudsters know that there is little chance of actually being caught once the voucher is found to be inactive, compromised, or even counterfeit".

From a card manufacturer's perspective, in broad terms unpersonalised base stock is printed using both lithographic and flexographic print disciplines and can be produced on both web and sheet fed presses.

The 'cut single' ISO card route employed by Atlantic Zeiser 'Cardline' type suppliers takes pre-printed and pre-cut base stock and feeds card bodies in single file down a track at high speed, typically 25-30,000 cards per hour. The numbers unique to each card are applied in sequence from a pre-loaded data file and verified by camera prior to the application of the scratch off product further down the line, again under camera supervision. Scratch off in this environment is either label or hot stamp foil. Cards are then collated at the end of this process and advance to the wrapping stage. The labour content in this environment is quite low, thus containing a significant element of cost for the supplier.

ISO format cards produced carrying silk screen latex panels are usually personalised in sheet form from lithographic pre-printed base stock. The data panel is usually hit with 2 or more layers of scratch ink and then overprinted with a security pattern, usually bleeding over all 4 edges for additional security. Cards advance to the wrapping stage after checking, cutting and profiling. Labour content in this environment is usually more complex, due to the increased number of production processes involved. However, quality and aesthetics of the finished card stock is usually high.

The third broad production process applies to the high speed web fed flexographic process, where card stock can be printed, personalised and protected in one continuous process, depending on individual machine specifications.

While this process tends to favour the non-ISO formats, a number of enterprising suppliers of machines in cooperation with card manufacturers have adapted or developed solutions to produce very cost-effective ISO format cards using this production route.

One such machine supplier is Edale Limited, based in the UK.

Edale's Head of Sales & Marketing, Jeremy Westcott told 'Product & Image Security' during a recent discussion, "Edale supplied its first phonecard production machine into Australia in 2001, and since then we've made further installations all over the world, including the emerging markets of Nigeria & Vietnam".

Jeremy continued, "There is a large amount of interest for these systems in the security markets of Africa, India and South East Asia due to the high population density in these parts of the world and low levels of personal bank account usage. Prepaid scratch cards provide an easy way for people to use their mobile phone with the credit paid for in cash rather than any form of electronic top up more normally seen in the developed world".

The current generation Edale system is capable of producing in excess of 1.2 million cards per shift, with the next generation set to produce more than double this quantity. The addition of special options allows the line speed to be greatly increased as well as improving press-ready set up. "It is no surprise that we have a high level of interest from these markets for this system", Jeremy added.

In line with the third type of production methodology

detailed above, the Edale system works in an entirely flexographic environment for base print and scratch off zones. The variable data is applied by thermal inkjet cartridge technology. Jeremy told us, “This system enables excellent flexibility coupled with fast changeover time between print jobs, enabling printers to produce multiple jobs in a very efficient manner”.

“Added benefits include the development of strong relationships in the areas of security inks and inkjet technology to enable us to offer a full solution spanning capital equipment and consumables which enables our customers to buy with confidence and removes the issue of managing a number of suppliers internally. We believe this approach enables companies to concentrate on customer development, drive out cost and retain confidence in their production capabilities”.

This modular system provides great versatility, enabling the press to be adapted to different levels of security requirements necessary for different customers. “We know customer requirements vary greatly, and this press can accommodate many different substrates ranging from carton board up to 600 micron styrene, all while ensuring security and quality”, Jeremy concluded.

Martin Horn told me simply, “Many manufacturers use Atlantic Zeiser technology, which limits them to producing variants of the 86 x 54mm ISO cards. At Securi-Tech, we use bespoke machinery, which gives us much greater flexibility in sizes and formats and facilitates more efficient logistics to lower Telecoms Operators’ distribution costs”.

Irrespective of manufacturing route deployed, Praesidium’s Simon Collins notes that, “A critical part of ensuring security of the product during the manufacturing process is for operators to ensure that stringent security and quality audits are undertaken; the focus being to validate that manufacturers operate in line with stringent security standards and that practices are actually evidenced to the auditor.”

“We at Praesidium have undertaken numerous security audits of prepaid voucher manufacturers globally and we’ve witnessed varying levels of security measures incorporated within the production facilities. The problem is that there are no recognised telecoms industry standards for voucher production and this is where specialist consultancy can support both the vendor and the networks they supply. Our service provides manufacturers with the confidence that their facilities are protecting the interests of their clients and delivers a benchmark on the level of security standards against the world’s leading manufacturing facilities. We also believe it serves to demonstrate to the network operator that vendors have a defined level of security protection to their prepaid product”, he concluded.

## What security features do they carry? Why?

As we’ve already discussed, a recharge voucher is effectively a network’s own currency, and therefore needs to be protected from fraudulent or counterfeit activity.

Features deployed can be both overt & covert in their nature and there is no ‘silver bullet’ answer as to what is right or wrong. We’ve already discussed key areas such as substrate and scratch off protection, and in truth these areas account for the vast majority of on-card security.

It shouldn’t be possible to delaminate, or separate, the board to enable to PIN code to be compromised, and ideally the board should contain a coloured centre to inhibit the passage of high intensity light through the card. The box area onto which the unique data is applied should be protected with a cocktail of inks to create a confusion panel and scratch panels should be specifically opaque enough to provide full integrity.

Simple print features like micro-text and UV inks could be employed, but as the card needs to be verified at the point of purchase, often in the hustle and bustle of a city street, these features are not really appropriate for immediate analysis, rather being a back office function and by then it is too late.

In real terms, the card must be readily identifiable as legitimate to the consumer, and this means the physical features we’ve already talked about. Overprint on the scratch off area, a holographic hot stamp foil or non generic label are the key areas to focus on.

"The first key issue is PIN security", says Securi-Tech's Martin Horn. "The second is resistance to copying and counterfeiting, which is achieved by a variety of methods. Overt methods include the use of UV inks or overlaid patterns in UV varnishes. These are primarily to deter simple photo-copying by low-level fraudsters. Covert features include micro-printing and other items not visible to the untrained eye. These can then be used by suitably qualified specialists to distinguish genuine from fake cards, in the event of a more sophisticated mass counterfeiting attempt. However, due to the inherent security of the telecoms operators' back office billing systems, the opportunity for fraudsters to make significant money from mass-counterfeiting is so diminished in many markets that clients no longer require these extra cost features".

John Drinkwater says, "From a manufacturer's viewpoint, and assuming all these areas are achievable, much of the security comes from the unique number control and traceability of the cards using the network's and the manufacturer's IT, all the way down to single card tracking level if needed".

Praesidium's Simon Collins sums it up this way, "There are a number of security features which can be incorporated into a voucher's specification and overall design. However, these usually incur higher production costs and operators' budgetary constraints, or lack of consideration to security, mean features are not readily incorporated".

"The key point, I think, regarding security features is that they're tested and validated to ensure their effectiveness and that the introduction of a security feature doesn't result in the overall design becoming insecure. Varying degrees of security protection can be applied, but in reality networks need to evaluate for themselves what the level of risk is in their particular market. This approach may allow operators to vary the level of security and amend features as and when to counter the fraud risk".

Abdul Mia put it succinctly when he told me, "Whatever you do and however you do it, only one thing is important and that is to ensure the card is resistant to fraud".

## Data transfer, application and integrity control – how are these achieved?

Data is the DNA of the scratch card and is where the millions of dollars of airtime revenue is contained. It is provided to the vendor in encrypted form, the complicated algorithms a closely guarded secret.

Until recently, and from my own experience, data files were burned to disk in the country of origin and despatched via any one of a number of international couriers to the manufacturing partner, usually in a separate country. This involved not only delay in receiving the files, but there was also the risk of the package failing to arrive, or arriving in a damaged state. Data files could be corrupted or having missing number ranges and these issues invalidated the data requiring it to be re-sent, causing further delay and re-scheduling of production in extreme cases. Passwords would normally be sent by SMS.

More recently, networks have started to deposit data (and artwork files) in sFTP (secure File Transfer Protocol) sites with secure login procedures hosted by the manufacturer. These 'electronic mailboxes' clearly enable real-time transfer of information and accurate and speedy response times from the vendor to any issues encountered with such data receipts.

Praesidium's Simon Collins told us, "The key aspect from a security perspective is that the network operator is assured that the PIN code data is securely encrypted, transferred and managed by the vendor under strict data and information security requirements, normally in line with internationally recognised standards. Auditable controls and processes must be in place at both ends to ensure 'closed loop' data management of the PIN code files".

He continued, "This must encompass the PIN code transfer and encryption process from the operator to the manufacturer, internal transfer to the production environment, storage and destruction processes. There should be a robust re-make procedure in place in the event of card spoilage to avoid duplicates and missing cards from the sequence, and at each relevant point the parties should be able to demonstrate that security is in place and this should be part of any planned auditing".

"We deploy our own bespoke software to securely process PIN and serial number data and to create comprehensive packaging, labelling and auditing data", says Martin Horn. "This system allows for output scanning and complete closed loop control".

Abdul Mia is a little more guarded. He told us, "Each vendor has different ways, but there needs to be some standards. The problem is that there are too many vendors around, and operators should make regular visits to check that all the security that suppliers say is in place is actually there".

As we said earlier, it is particularly important to have internationally recognised credentials and more and more networks will only work with vendors who have these in place.

## Card packaging – which methods provide the best security against theft or card attack prior to final consumer use?

Before formats changed to include the newer non-ISO card variants, packaging of recharge cards was pretty straightforward. Cards were simply individually flow wrapped in either clear or printed BOPP film, pretty much like a chocolate bar, down commercially available flow wrap lines before being collated and labelled in batches, usually 10 cards per batch and 10 batches per carton. 10 cartons were then further boxed in shipper cartons and labelled before final transit packaging such as pallets or wooden crates. What we basically had was an easy to follow trail of hierarchy (1-10-100-1000). There were unique variations on a theme, but this was basically the template for card packing.

High speed wrapping lines for ISO cards were introduced a few years ago and a range of suppliers developed broadly similar solutions, including Germany's Atlantic Zeiser & Köra-Packmat as well as Italy's Ilapak.

These solutions enhanced what had gone before, but provided new thinking on card packing. Instead of cards being wrapped individually in 'candy wrap', these solutions enabled cards to be fed into fast moving continuous pouches in a 'string' configuration before being cut at variable string lengths to suit individual specifications. The strings would then be collated into a 'z-fold' single card footprint before being over wrapped and batch labelled. The net effect of this was to radically improve output speeds of finished cards while enhancing the numbers of cards per pallet or crate, thus reducing freight costs.

Some of these solutions employ an ultrasonic seal process, positioning the seal very close to the card edge and with the additional optional bespoke sealing bar carrying a unique impression on the seal, such as the operator's name and / or logo, this makes for a very secure package.

In certain cases, operators have forgone the individual pouch and elected to pack lower denomination cards, usually carrying multiple PINs directly into the outer batch wrap. This does make some sense from a cost perspective, but also from a stock management viewpoint. In order to sell a section of a full card body (as it is not usual to sell all the PINs on one body to one customer) it is necessary to remove the card from the packaging and therefore the additional individual film layer becomes a costly extra that can be dispensed with. At this final point in the distribution chain, it is not unusual to see cards already de-bagged and broken into individual sections, such is the demand for these products at peak times of the day.

Abdul Mia comments, "For me, packaging of the batch should be 10 cards or for higher denominations packaging should be in singles. The wrapper must have a snug fit so it is easy to spot if the card has been removed before sale. If it possible to have a wrapper that is destroyed totally on opening, then this is the better solution. An added feature could be to have the logo of the network printed onto the package, but this would be an additional cost, and here again the cost versus benefit argument appears. Operators need to assess how many of these cases they get and whether it justifies the extra cost".

The impact of the newer low cost formats has seen some alternative thinking to these products. Designed to be quick turnaround and high volume, high repeat purchase products, packaging has adapted to meet these benchmarks.

In certain cases, the 'bricks' of vouchers are not wrapped at all, merely sleeved in sequential number and labelled with the number range and other key data before being bulk boxed and despatched. While the product doesn't downscale the data integrity on the voucher itself, the 'budget' nature of the product dictates a lower specification of packaging. In many cases, the airtime reload value is so small per individual voucher section that it is not worth the fraudster's time to attempt to compromise these cards when the higher value cards would occupy just as much time in doing so.

In other cases, and as evidenced by a number of operators, cards are flow wrapped in the traditional way in multiple sheets per pack with individual numbers of sheets per pack being decided by networks individually.

In all cases, it is important to understand that the market dictates pack quantities, not manufacturers, as it is all about 'pack value' through the supply chain. It is important that integrity is maintained right up until the individual packs themselves are broken open, and at this level the sub dealer of the sub dealer needs to be able to afford to buy his stock.

What we need to understand here is that the network can only sell its airtime once. This is to a select group of 'super dealers' who are incentivised with volume discounts or directly through its own retail channel. Super dealers then feed the remaining secondary, tertiary and beyond network of re-sellers right down to the street vendor. It is at this very level of the supply chain that the dealer must be able to afford to buy the minimum unit of issue or the system breaks down. Of course, cards can be sold at any time to a consumer in this process, but the bigger dealers are more flexible in this regard.

What we experience in many cases is significant effort being applied at the manufacturing end to ensure robust packaging and wrap security for this to be obliterated in the market place.

Simon Collins told us, “In our experience the best type of voucher packaging uses an ultrasonic seal for individual vouchers. Ideally the seal should be as close to the edge of the card as possible, so that when the voucher is removed it shows visible damage to the packet. This prevents the card being removed, compromised and replaced. Additional measures to incorporate the operator’s name and / or logo in the seal can be deployed, although at extra cost”.

“Secure tamper-evident tape should be used on transit cartons to prevent tampering during the distribution process and ideally the outer box or pallet should not display the exact contents to avoid opportunistic theft”.

Martin Horn again, “At the higher levels of packaging, such as the batch box or shipper box level, it is vital to use tamper-evident seals to ensure that the boxes have not been opened in transit and some of the contents stolen”.

“However, wrapping at the card level should certainly not be a necessary security element in protecting against card attack. To expect otherwise is to fall prey to a similar ‘faulty’ logic as that concerning the use of black core paper as I mentioned earlier. Any kind of wrapping can be repaired or replaced by a fraudster, so it is far more prudent to employ card technology that ensures that unwrapped cards are already inherently secure. The need for this is even further underlined by the now widespread use of strip cards and multi-part ISO cards where there are multiple scratch panels within one wrapping. Unsold scratch panels need to remain secure after unwrapping. Securi-Tech therefore regards any kind of card wrapping as simply a protection against dust, dirt and moisture in transit and we certainly do not consider it a security feature”.

As with other areas of this discussion, there is no right or wrong way to look at this. Operators and manufacturers have to constantly balance the security, risk and cost factors in their card programmes and to a degree decisions made by one network versus another will vary, even in the same country.

## Card imports – what are the freight implications of transporting high value documents? What can freight companies do to ensure secure transportation from point of manufacturer to the client’s nominated destination?

While there is a move to localise supply in many markets, it is inevitable that cards need to be shipped from one country to another where networks continue to specify external suppliers.

It isn’t sufficient to expect general carriers to handle this type of product, particularly after all the effort that goes into producing it in a secure environment initially and the onward warehousing and distribution surrounding the product when eventually passed into the operator’s custody.

Praesidium’s Simon Collins again. “We take the view that vouchers are effectively cash and appropriate security measures should be implemented for the transfer of goods through the distribution chain. Auditable processes must be in place and any evidence of tampering of goods must be notified to the manufacturer and operator”.

“Obviously, the degree of protection varies from country to country ranging from a basic courier service to the deployment of armoured vehicles and the level of security needs to be weighed against the actual threat level. Also, consideration needs to be given to the value of insurance cover that will be provided for the goods in transit to ensure the correct level of cover is applied”.

From the network operator's perspective, Abdul Mia shared his thoughts with us on the related subject of card distribution from warehoused stocks. "What I found very helpful and a workable solution to the movement of cards into the market was to incubate the cards in an inactive state while in the warehouse. We also kept them inactive during the delivery to the super dealer as if the cards went missing in transit they would have nil value. The super dealer would then send an activation request either on receipt of delivery into his warehouse or later when sending cards out to the sub-channels".

"The operator only has a relationship with the super dealer and so he should be the only one to send an activation request. He can have a further process with his dealers further down the track but he should only interact with the operator".

"Securi-Tech offers its CHKVOUCHER solution to secure and track cards from our premises through the distribution chain and even all the way to the final retailer, if required", Martin told us.

"CHKVOUCHER is a real-time online service that can be used to manage card states as active, inactive, in transit, in warehouse, lost, stolen, etc by scanning ranges of cards in and out at various points in the supply chain. In this way, each card is always traceable".

Peter Reynolds, Managing Director of Artac Logistics Ltd, a specialist forwarder of sensitive and valuable freight based in Southern England told 'Product & Image Security' during a recent wide ranging conversation, "Artac offers a comprehensive range of airfreight products to meet our customers' needs, all supported by the latest IT systems and track and trace facilities. Airport to airport or door to door services, regular consolidations worldwide, urgent express movements, courier services and import customs clearance form part of our day to day activities".


Peter continued, "Additionally the provision of all necessary documentation ensures the smooth transit of the client's consignment including consular documentation, insurance and letter of credit compliance. In addition, we offer a range of ancillary services associated with international air transportation including a nationwide collection and delivery service, x-ray screening for unknown cargo, packing services incorporating hazardous packing under guidance from our own DGSA and customs clearance at all major UK airports".

"We currently work with a number of UK security printers and component suppliers, as well as businesses located overseas so we're fully conversant with the demands of shipping secure freight in 'closed loop' situation, including into less stable parts of the world. Whatever the airfreight needs, Artac has the right solution to ensure its clients' goods are safely transported and delivered on time to their destination through a choice of reliable, cost effective services".

"Artac is also regarded as one of the leading air charter brokers in the UK, so we're well placed to provide our clients with the best possible service and advice to provide aircraft to meet specific requirements on a global basis. This could be for a consignment of a few kilos or 250,000 kilos airport to airport or door to door".

"Aircraft aren't always chartered for rapid response and emergency needs. They frequently provide a competitive and effective method for transporting goods for arrival on a specific date/time which may not be possible with scheduled airlines".

"Using charter aircraft can assist with planning, storage, distribution and can prove cost effective. In addition to providing dedicated charter aircraft we also offer part charters and' empty legs' which can reduce costs. Aircraft of all types including helicopters are operating on a global basis. Artac maintain an extensive data base to ensure whatever the load / routing, we will provide the best solution and price".

"We're members of IATA and are a regulated Department for Transport agent compliant with aviation security regulations", Peter continued.

"If the client needs to ship by sea then Artac Logistics' seafreight activities include NVOCC services and world-wide forwarding, specifically designed to meet the needs of each individual customer", Peter told us.

"In association with our network of overseas agents Artac Logistics can provide importers a complete logistics package, arranging carriage from suppliers through to delivered customs cleared. Shipments are monitored throughout, thus offering greater control to its customers. Whether your business is export or

import, Artac Logistics can provide a total transport solution".

"We offer all our customers approaching the world of international trade for the first time or breaking into new markets the benefit of guidance from our dedicated and experienced staff, who are able to attend to all necessary documentation to comply with banking requirements where applicable".

## What are the main risks associated with using the cards? From a user perspective? From a provider perspective?

Abdul Mia's view is that it breaks down into two key areas. "For the user it is about theft or loss, and for the network it is about the costs of running a card programme, particularly in production, warehousing and distribution terms".

John Drinkwater thinks along similar lines from the user's perspective. "If I was a customer, I'd be wondering if the card was genuine and is my money safe. I'd be concerned if the number had been accessed or used before I bought the card".

"Wearing my industry hat, I'd be proposing tamper evident scratch panels to the network or their suppliers, based around high opacity holographic foil for public recognition security. Labels less so. They can be lifted and the numbers accessed, although I concede that they're better at preventing over-scratch".

Simon Collins has the following views. "From a user's position, the risk is mitigated to some degree because if a customer finds that the PIN code has been compromised, or there is an over-scratch issue, then most operators or the point of sale will usually replace the voucher or load the airtime remotely via a customer service centre. However, from a commercial viewpoint this isn't viewed as good customer PR as subscribers lose confidence quickly in the product, and there are rival networks available".

"The risk for networks", he continued, "is far higher as a security incident where the PIN code is compromised, or a large number of complaints over security are received would usually mean the network losing faith in the supplying manufacturer and potentially cessation of supply and legal redress. Alternatively, the network could demand the whole production run is undertaken again, or that they're financially compensated which would be a huge financial exposure for the manufacturer".

From the card manufacturer's perspective, "The risks depend on the quality of the card product as I mentioned earlier, and the security and reliability of the card manufacturer's physical and data processes", says Martin. "To date not a single incident of fraud has been reported by any of our clients in connection with Securi-Tech prepaid cards. In addition, our new Tuff Voucher technology significantly reduces the risks associated with over scratch for both the telecoms operators and their consumers".

## What forensic testing takes place? Is this done internally or via external laboratories?

In my experience, forensic testing procedures are deployed right across the spectrum of the industry from card manufacturers with in-house laboratory facilities through to personnel specifically employed by networks in Revenue Assurance and Fraud departmental positions and on to 3rd party specialists and consultancies.

It has also been my experience, and that shared by some of our contributors that the approach to this area, as with other areas, is not uniform or consistent. In certain cases, manufacturers have been pilloried or placed under great pressure by networks to meet arbitrary standards while other suppliers have not been subject to the same examination.

Reputable manufacturers in the main have at least some in-house facilities and in certain cases they work with specialist consultancies to 'health check' the internal results. Such tests can include abrasion testing, sophisticated light show through tests at various points on the UV and IR spectrum, climate testing and so on.

"For example", Martin Horn told me, "Securi-Tech has its scratch cards independently tested by a special unit within a university department's Polymer Sciences laboratory using a range of high-tech equipment to test security including lights, lasers, x-rays, ultrasonics, infrared and microscopes. In addition low-tech attacks with adhesive tapes, solvents, knives, etc are used to simulate the environment where cards are used at street level. In addition, the laboratory tests the cards for scratch-ability and for resistance of the PIN to over scratch by various methods".

Jannie Bester from Pro Scripto told me, "I've been doing vulnerability assessments on physical recharge cards for the past seven years, and during this period I've assessed many thousands of cards for various networks, card manufacturers, and card component suppliers worldwide".

"We look at opacity, scratch off characteristics, counterfeit vulnerability, covert security features and mechanical access to the PIN code. We assess

according to the 'reasonable man' test and this doesn't involve expensive equipment, but rather cost-effective equipment available to the reasonable man".

"I've also developed a custom scoring system to measure recharge card technical compliance with the network's specifications, and during the past seven years, I've also developed forensic methodology to examine counterfeit vouchers and gather forensic technical detail for expert forensic document examination evidence regarding authenticity issues".

Jannie continued, "Some manufacturers tend to over-emphasize security issues and skew the balance between cost and security. Networks don't always have the technical skill with regard to accurately specifying the technical characteristics of a recharge voucher, and they rely on manufacturer recommendations without having these reviewed by an independent entity or get an independent consultant involved in the procurement process. I'm of the view that this in itself exposes the network to various risks which can impact directly in the bottom line".

"We were able to save one of our clients multiple millions of Rands by being involved in this process during the past seven years".

Abdul Mia told me, "Most vendors claim that they do such tests internally, but as an operator I wouldn't want to rely solely on their results. I would want operators to use reputable external laboratories".

"in my experience I've seen several ways in which PIN codes can be compromised, such as by UV light, extreme light, photo-copying, tape lift, solvents and theft of PINs from the computer system before they made it onto cards. This included removal of the PINs from the vendor's system or from the disk despatched to the vendor, internal fraud within the network and theft of PINs during the production process itself".

"I combated many of the compromises by ensuring vendors were regularly tested by a reputable agency. For example, in South Africa we used a university. This made it much easier to shift the blame back to the vendor in the event of compromise and made cost recovery more straightforward".

"We also did regular inspection visits of our own to ensure our vendors' security measurements were adequate and we often tested these systems. Amazingly, we found many issues despite assurances to the contrary".

"Finally", Abdul said, "we instigated contract clauses with our suppliers that they invest in R&D on the products and keep us informed of new products or techniques that would assist us in combating different types of fraud, especially ones that had been encountered with that particular vendor before".

As a former GSM Africa Fraud Forum Chairman, Abdul remains keen to see some standards across the industry implemented by the GSMA, similar to the SAS scheme (SIM Accreditation Scheme). "I'm very passionate about this", he said, "and I've tried for a long time to introduce something similar into the recharge card area. But the problem with this is that there are too many players in the market, and markets like Nigeria have regulations as to who can and can't produce cards for the local networks. This makes it difficult to implement some decent regulations, but I still believe there is scope for this. Some efforts have been made and there is some headway, but there is still a long way to go to get this right".

Simon Collins from Praesidium told us that security and quality testing of prepaid vouchers for manufacturers and networks is a key area of work for the business. "Our service is aimed at providing manufacturers with a benchmark relating to the security and quality standards of their own product with those offered by other leading suppliers. We base our findings on a number of key security and quality related testing scenarios developed in-house".

"They vary in nature, but include:

- Artwork review – to determine the colours used, positioning of the diffusion panel and the ease with which counterfeiting could occur
- Voucher body – evaluation of the actual material being used and the specification – plastic, paper, thickness and opacity
- Physical protection – assessing the physical protection of the PIN code relating to numbering, spacing, scratch off panel integrity and 'remove and replace' type attack opportunities
- Specific testing – subjecting the vouchers to a number of specific tests involving: light sources of varying intensity and wavelength; heat, steam and cold in varying conditions; solvents and adhesives; inherent security measures (specific product features); scratch panel adhesion and quality; brute force attacks
- PIN code printing – assessing printing effectiveness to identify how many PIN code digits can be identified based on the various testing scenarios from partial to full reveal.

- Production quality – assessing the production quality to determine consistency within the product being produced

- External packaging – evaluation of the external packaging to test against the feasibility for 'remove, compromise and replace' techniques"

John Drinkwater concurred with our other experts' views on what the industry should be testing for, although he had this to add to the debate. "Most plants have developed their own tests to use internally, but most major networks tend to use outside technical specialists occasionally".

"There are some outside testing forensic agencies offering services in this area to varying standards although it is important they remain impartial between techniques and suppliers to avoid distorting the market. It is also important that they use techniques that reflect 'real world' challenges in the market place".

## What is the future for prepaid airtime reload cards?

As we've seen from earlier comments, the physical card has been a mainstay of prepaid recharge for many years and our experts see no reason for that to change for some years to come.

Until infrastructures in some of the developing world catch up with more advanced economies, then the scratch card will continue to play its part. The unquenchable thirst for mobile communications in these parts of the world shows no sign of slowing down, and while other technologies nibble away at its place at the table and the format may evolve and change, no other method of recharge can offer the depth of marketing opportunities for networks to tap into their customers' requirements.

We've not even fully considered what other applications the physical card may have. In cash based economies and where other services are required, such as power and water, there may be additional opportunities for the scratch card in these utility areas. After all, the mobile phone when all is said and done is another utility service. It is just that the fruit in this area hangs much lower for providers.

As Abdul Mia says, "These will be in developing markets for a long time to come". Jannie Bester concurs with this view, telling me, "Recharge vouchers have a good few years left yet".

Martin Horn agrees. "As I've already said earlier, secure scratch cards still fill many slots in the airtime distribution model which cannot be adequately serviced by other methods, especially in developing markets. At this stage, overall card volumes are still growing; particularly in the case of low denomination values. As telecoms operators increasingly use micro-recharge offerings to penetrate deeper into these markets, the numbers of scratch cards they use continues to grow. As a consequence, the telecoms operators also seek to control their costs by continuing to drive unit card prices lower".

"I therefore foresee a scenario where lower volume scratch card manufacturers might cease to be viable, especially given the significant security, IT and quality-related overheads necessary to produce reliable scratch card products. Therefore, some fall-out and/or consolidation amongst the scratch card manufacturers could well occur".

And the author's view? I hope so…it's where I earn my living.

After a domestic UK sales career spanning 16 years in print & paper conversion, Nigel Page has since 2004 specialised in international sales & business development primarily into the telecommunications marketplace. Having spent the majority of this period to date with one of the UK's leading security printers in its dedicated Telecoms Unit , Nigel is an expert in his chosen field. The initial article and subsequently enhanced White Paper, commissioned by Product & Image Security Magazine in early 2010, is the result of not only Nigel's experience and insight, but also that of the many and varied contributors, all industry specialists & colleagues, who supported this investigation so admirably.

A UK national and resident, Nigel is an Associate Member of The Institute of Export and can be contacted as follows:

E.Mail: nigel.page@sky.com

LinkedIn: http://uk.linkedin.com/in/nigelpage

Telephone: + 44 7778 771 848