

Prepaid Voucher Security... Risk Free?

// Very few operators are giving sufficient thought to the risks that are prevalent within prepaid voucher production //

Prepaid was initially viewed as a “no risk” product. The financial risk was reduced as there was no credit management required and no overheads for billing customers. In today’s telecoms markets, Prepaid has become the biggest revenue earner for many operators.

Præsidium’s experience is that very few operators are giving sufficient thought to the risks that are prevalent within prepaid voucher production. Most operators these days use one or more third party vendors (manufacturers) to produce the vouchers. In some instances, these manufacturers are in the same country whilst in other situations the manufacturers are thousands of miles away. Irrespective of the geographical location, exactly what are these manufacturers producing? The harsh reality is that operators have selected the preferred vendor to “print cash”.

Are you fully aware of what this manufacturer is actually doing? What standards of security are being afforded to your data and vouchers?

Regrettably in the majority of cases the answer is “NO”, operators have no real comprehension of what is actually taking place. This brings us to the interesting perception relating to the type of companies that are offering such manufacturing facilities. Secure voucher production is still a relatively new industry. There are very few specialised voucher manufacturers in the world. The majority of manufacturers have adopted similar production techniques, which have evolved from credit card manufacturing or lottery ticket production. Whilst there are similar processes involved, the production process is very different and requires diverse security management techniques.

Example 1:

Lottery ticket manufacturers often have well established and excellent production techniques, however, out of the thousands of tickets produced, less than 1% will ever be a “winner”. However, with

Contact Details:

Præsidium Services Limited
Atlantic House
Imperial Way
Reading
RG2 0TD
United Kingdom

Phone: +44 118 922 4444
Fax: +44 118 922 4432

admin@praesidium.com
www.praesidium.com

praesidium

voucher manufacturing “every one” is a winner. Therefore voucher manufacturing demands an increased level of security.

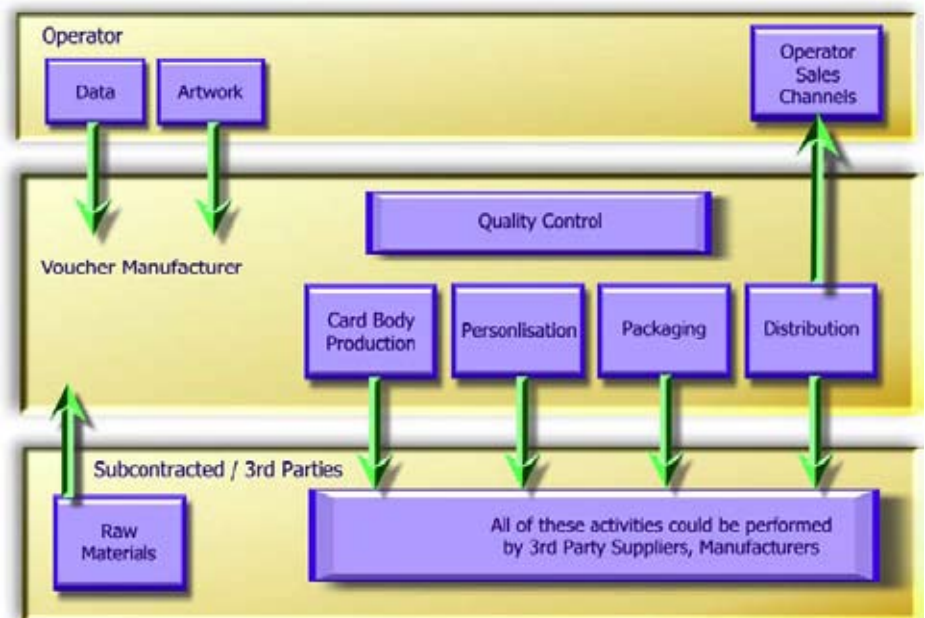
Example 2

Credit card manufacturers are well aware of the risks involved with data protection and manufacturing security, however, credit cards do not normally require packaging. Whereas, with vouchers the packaging is just as important as the physical voucher itself. If the packaging is weak then the card may lose up to 50% of its protection and provide unnecessary exposure to fraudulent attack, e.g. remove and replace.

Another key aspect to appreciate is the unforeseen risks associated with manufacturers using subcontractors in the voucher production process. This is often unknown to the operators and in some instances directly in contravention of the contractual arrangements. Voucher manufacturers are increasingly using subcontractors for areas such as art/ design work preparation, personalisation, scratch panel printing, packaging and distribution, which are the essence of ensuring a secure product is being delivered.

Do you know who is “actually” producing the different elements of your vouchers? Have you ensured that end-to-end security for all these companies has been implemented to protect your data and products?

There are 8 main areas for voucher manufacturing security that need to be adopted; these are shown in the diagram below.



The diagram summarises the main risk areas associated with voucher production. This, however, does not include areas relating to physical security, emergency procedures and business continuity. These important areas will always be different depending on the physical location of the production facility and the vendors overall business strategy for ensuring a continued production capability. The risks associated with these areas are similar to those experienced by many telecom operators when protecting key network buildings or

warehousing facilities. These areas must be incorporated in the overall security risk assessment.

Raw Materials

Components needed to manufacture vouchers are generally sourced from preferred suppliers. In general these suppliers will only supply "sensitive" products to recognised voucher manufacturers, however, there will always be exceptions. The protection of raw materials needed to produce your specific vouchers is vitally important. The criminal fraternity may be able to duplicate the artwork of a card, but sourcing or reproducing the exact scratch panel should be more complex. The easiest solution therefore is to acquire this direct from the supplier or voucher manufacturer.

Præsidium has witnessed few manufacturers having the appropriate levels of protection in place regarding the secure storage of raw materials. This coupled with an inability to correctly quantify or account for the amounts used presents a dangerous combination to the operator.

Do you know who provides all your materials? Has the security of the scratch panel ever been tested? What controls are in place regarding the security of these products?

Data Protection

This represents the most significant risk exposure to fraudulent attack and as such demands the highest standards of protection. Data theft can occur at the telecom operator, in transit or from the manufacturer's IT and production systems. Præsidium has witnessed manufacturers concentrating on ensuring that "visible" security is in place (e.g. access control CCTV cameras, vaults etc.), the "invisible" security is often lacking. Leading international manufacturers have dedicated IT Security Managers and secure local networks. However, lesser known national manufacturers do not have a dedicated resource nor possess the required expertise to manage or understand the associated data integrity risks. Præsidium has identified many instances of commercially sensitive historical data being held insecurely or the data has never been deleted from the systems. Manufacturers therefore have millions of PINs (Personal Identity Numbers) or HRNs (Hidden Recharge Numbers), the monetary value of which represents a substantial risk should this data be compromised due to a lack of data security.

Præsidium has seen several cases around the world where internal fraud, negligence or weak protections have enabled data to be obtained. In one case, millions of HRNs were left unprotected relating to a number of operators who all believed the security in place was at an acceptable level.

Do you have confidence in your manufacturer regarding the data you have supplied? Can you be certain that at all times data is being securely handled and deleted in accordance with your instructions? How confident are you that your data will not be compromised internally or hacked externally?

“ In one case, millions of HRNs were left unprotected ”

// Præsidium is seeing increasing activity relating to high quality forged / counterfeit vouchers ... in many instances only a trained eye is capable of detecting the fake //

Artwork

In today's technological world, even young children are capable of modifying and copying graphics and have at their fingertips a myriad of different photo and graphical software packages. This is increasingly true of fraudsters operating within the telecoms industry. Previously most forgeries and counterfeit products were in relation to money, credit cards, consumer goods, watches and the fashion industry. Præsidium is seeing increasing activity relating to high quality forged/counterfeit vouchers. In Russia 3m fake vouchers were produced. Everything from the artwork to the scratch panel could be re-fabricated and in many instances only a trained eye is capable of detecting the fake, so what chance does your customer have?

Example

Work undertaken by Præsidium in Scandinavia highlighted thousands of counterfeit vouchers that were "perfect" copies of the originals sold by the operator. The only way these vouchers were identified was the counterfeiters produced the vouchers with the same visible serial number and HRN. In every other way, including the scratch panel, the voucher was an exact copy, which also included the voucher packaging (film wrap).

Why did the counterfeiters make such a big mistake with the HRN? Or were they just testing the market prior to a concerted attack!

Although some of the leading voucher manufacturers now provide advanced anti- forgery defences (including holograms, heat sensitive panels, ultraviolet designs, microprint etc.), these can often be expensive and will increase the manufacturing cost per voucher. A business decision is required to evaluate the risks prevalent within the market environment against the necessary protection of the HRN.

What protection does your voucher body provide? Have your vouchers been tested to ensure that the most common techniques for compromising the "secret number" can be avoided? What assurances does your manufacturer provide you? What does your contractual agreement say relating to fraud?



Voucher Body Production

Traditionally paper "fold-over" designs were used by some older operators, or those wishing to cut manufacturing costs. These have been rapidly replaced by the more common "plastic" card body variety; both types have some inherent security weaknesses. In order to reduce the production costs, operators are choosing a laminated paper voucher, which is similar in design to the plastic variety but is often much thinner/ lighter and cheaper to produce.

Each type of voucher body has its own strengths and weaknesses and in the majority of cases will have been selected based on the "consumer look" and cost of the product, not the security requirements to protect

the operator's revenue. Very few operators seek assurances from the manufacturers regarding the tests performed to ensure the voucher panel cannot be exposed to simple remove and replace techniques. Operators should be asking about the testing scenarios deployed relating to the ability of the voucher body and panel to protect against different light sources, solvents and brute force attacks.

Operators must ensure that vouchers have been fully tested and evaluated. They should either seek this compliance from the manufactures themselves or use an independent third party (consultants, laboratories).

Personalisation

Personalisation is the most critical and sensitive part of the voucher manufacturing process. An operator effectively trusts the manufacturer to ensure the HRN is not compromised during this process. Depending on the types of machine used for personalisation, the HRN can either be completely hidden prior to scratch panel insertion or the HRN could be visible to employees working on the machine. The working environment and supporting business practices are an integral part of maintaining the integrity of the HRN and are critical to ensure this sensitive stage in the process is secure.



// The operator was unaware that vouchers worth millions of dollars were moving around the country with relatively no protection, with the HRN clearly visible //

Example

One vendor Præsidium reviewed, performed the personalisation process and scratch panel insertion in two separate geographic locations. The vouchers were personalised by the voucher manufacturer but subsequently sent to a third party to have the scratch panel applied. The operator was unaware that vouchers worth millions of dollars were moving around the country with relatively no protection, with the HRN clearly visible to another 3rd party logistics company.

It does not matter that the voucher is not active as the criminal fraternity know that one day it will be and simple testing of the operators network will tell them when a concerted attack can be undertaken.

Normally within the personalisation process quality checks are performed to ensure the HRN has been clearly printed and correctly positioned. However, this process presents several risks. It is common practice for manufacturers to be required to reprint vouchers that have failed quality control. Præsidium has observed that in practice, inadequate control techniques are in place regarding the number of reprints produced or that protecting against the possibility of producing duplicate batches of vouchers is weak. This means that unscrupulous employees could create duplicate orders e.g. one to send to the operator, the other obtained by criminals to sell on the black market.

// Poor quality product security is often the result of operators either rushing a product to market or not evaluating the security requirements correctly. //

Subsequent to the HRN printing process, (the secret number) there is the application of the scratch panel itself. This will involve different techniques depending on the manufacturer, but is normally a hot foil stamp insertion or different layers of "scratch off" paint. Again depending on the construction, materials used and diffusion panel design, different risks are prevalent.

Præsidium has reviewed some excellent scratch panel designs that are near impossible to defraud and require considerable skills, techniques and knowledge to compromise. Unfortunately, Præsidium has also reviewed numerous vouchers where the scratch panels can be defrauded very easily with simple remove and replace techniques. These attacks leave no visible signs of tampering and result in vouchers being returned to the distribution channels without the operator knowing the security protection has failed until it is too late. Such poor quality product security is often the result of operators either rushing a product to market or not evaluating the security requirements correctly. Without the appropriate testing and evaluation being performed, operators will continue to be faced with fraud issues and the emphasis must be placed on designing and using secure products.

Are you certain your vouchers are being personalised by the designated manufacturer? What standards of protection are in place to protect your operator specific data? How robust and secure is your scratch panel? What integrity tests has the manufacturer performed and is the security to the level you have specified?

Packaging

Just as important as the manufacturing process is the packaging relating to the vouchers and the overall product, e.g. voucher wrapping, security tagging, boxing, crating etc. This extends from film packaging and crimping designs



to paper varieties, wooden/cardboard boxes and crates used for distribution. Præsidium has witnessed many instances of petty pilfering where employees, distributors and even customs officers have removed vouchers from the distribution channel.

In some cases the business decision to cut costs on packaging can have serious consequences on ensuring final delivery of the expected product consignment. Many manufacturers will provide secure options for protecting the goods, but again this can increase the overall cost of production. Therefore depending on the market conditions and the risks prevalent, operators have to make a balanced decision between cost and protection.

Example

Præsidium reviewed one operator who was providing bundled prepaid products and the marketing initiative had not taken into account the fraud risk factor. "Live vouchers" were being produced in country A and

// distribution of vouchers carries with it the same risks as if the operator were transporting cash. //

sent for bundling to country B, C etc. with the SIM and handset. When asked about the security in place the response was – “what security?”

Is your voucher wrapping tamper proof? Would you be able to detect a ‘reveal and replace’ attack? How do you ensure you receive what you pay for?

Distribution

Depending on the strategy deployed, the distribution of vouchers carries with it the same risks as if the operator were transporting cash. Again, depending on the country and level of criminal activity, often different standards of security are applied. The distribution must take into account the transportation requirements from manufacturer to operator and the associated risks. This must incorporate the courier services used, physical transport, delivery and warehousing. Associated areas of insurance and indemnity liability will also need to be assessed where multiple parties are being used.

The final stage of the distribution chain are the actual activation timescales for the vouchers and the internal sales channel distribution practices. A number of operator specific criteria can affect these timings, but there is a need to fully evaluate the timescales versus the availability of vouchers to the customer. Præsidium has witnessed a number of security and business issues relating to this area and the security protection has to be balanced to meet the distribution and sales needs.

Example

Præsidium reviewed an African operator’s, delivery and distribution of vouchers: the delivery consisted of an open-backed lorry carrying the consignment from the airport with no security. When the goods required unloading to the secure warehouse, the operator’s security guards were nowhere to be seen. The Warehouse Manager actually recruited the labour from the street without giving any consideration to the value of the vouchers being delivered. All of this was unknown to senior management.

What level of security protection is in place with your deliveries? Who is contractually liable for losses in transit? What are your emergency procedures should the consignment be stolen? What business continuity strategy do you have in place – no vouchers = no customers which is a harsh reality?

Conclusion

Præsidium’s experience has determined that voucher integrity requires a comprehensive strategy to be defined incorporating end-to-end security management. This strategy starts with the protection of commercially sensitive data within the operator, through vendor production to distribution of the final product to the market place.

There is no recognised industry standard to guide telecom operators and many of the facilities reviewed have the security status determined by international financial or regulatory authorities e.g. VISA, MasterCard or lottery bodies. Therefore telecoms product security will

be a secondary consideration for deploying security. Few operators are actively ensuring that their specific product has all the required security elements in place and they are not evaluating the risks.

Præsidium has global experience of voucher product security having evaluated the standard of protection at over 20 production facilities. Præsidium works with the operator to ensure that the security protection being afforded to their specific product is maximised and tailored to meeting the operator's voucher management strategy.

Præsidium is an industry leading independent Communications Risk Management Consultancy, which specialises in Revenue Assurance, Fraud Management, Network Security and Business Continuity across the wireless, wireline and internet industries. Over the last decade, Præsidium has conducted consultancy assignments for more than 100 telecom operators worldwide and for a wide range of OSS vendors.

For further information, please contact us.