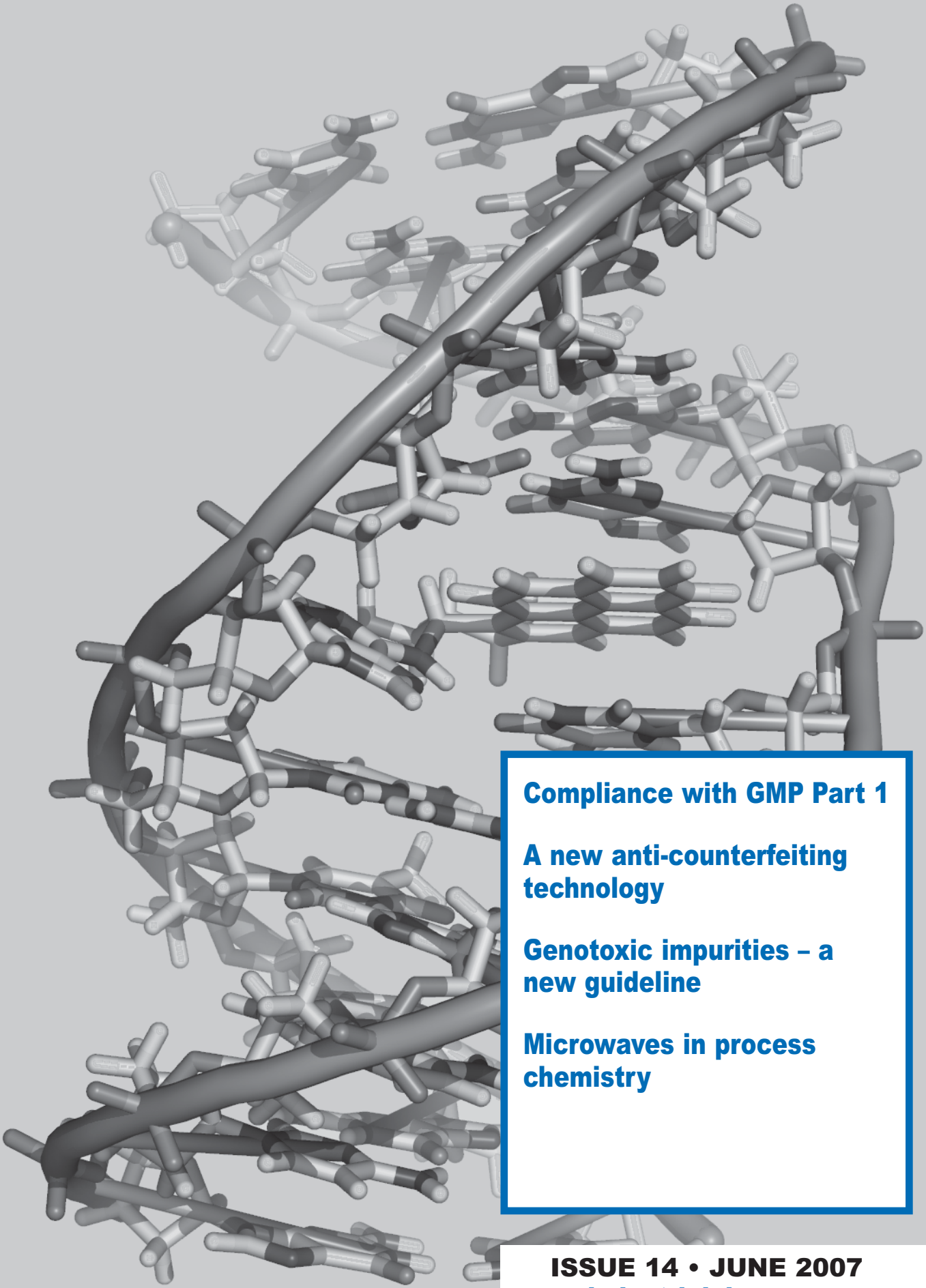
INDUSTRIAL PHARMACY



Compliance with GMP Part 1

A new anti-counterfeiting technology

Genotoxic impurities – a new guideline

Microwaves in process chemistry

ISSUE 14 • JUNE 2007
www.industrialpharmacy.com

Contents

FEATURES

REGULARS

Cover picture: Representation of a DNA double helix with a benzopyrene adduct – the first step in the process of DNA damage.

INDUSTRIAL **PHARMACY** is an official publication of the Industrial Pharmacy Section of the FIP

EDITORIAL

Fifty Years On... a personal glimpse

For pharmaceuticals, in some respects 1957 was a watershed year. Significantly for the UK industry, the British government managed, for the first time, to put a partial brake on companies' profits from their sales to the National Health Service by 'inviting co-operation' with a voluntary price regulation scheme. That single step became the forerunner to the now Pharmaceutical Price Regulation Scheme. As the scheme became more sophisticated over time, its sheer intricacy prompted a whole spectrum of reactions around the globe, from admiration to deep suspicion to plain bewilderment – and, to match all that, the familiar backhanded compliment: "Typically British". In the United States, the jury remains out even today.

Nineteen fifty seven was also a highly significant year on the research front. The discovery and isolation of the nucleus of penicillin, 6-amino-penicillanic acid was a classic instance of opportunistic inquiry and dogged pursuit of anomaly that typifies the very nature of pharmaceutical innovation. With corporate funds at hand, it enabled the development of a succession of formidable new antibiotics. And Albert Sabin's live attenuated oral polio vaccine demonstrated the enormous practical yet vastly underrated value of developing a convenient route of administration early on.

However, in the market place, there was little sign of change. Hallowed tribal practices continued unabated among the professions. In the UK for instance, by the time a prescribed medicines reached the patient, some if not all product identity was likely to have been obliterated during the course of the dispensing process – unless otherwise directed – and replaced with labels such as 'The Tablets', 'The Ointment', etc. Hence grew, with some justification, the commonly held belief that

PROTECTING PHARMACEUTICAL PRODUCTS FROM COUNTERFEITING USING DIGITAL IMAGING TECHNOLOGY AND OFF-THE-SHELF CAMERA PHONES

by Roland Meylan

New ways to protect pharmaceutical products against counterfeiting and other illegal activity are provided by new technologies based on software and digital imaging. Off-the-shelf consumer electronics and camera phones converged with secured Internet servers can now detect fake or re-directed product (grey market) anywhere and anytime. This new technology can be covertly and seamlessly integrated into package production without any hardware investment.

Pharmaceutical counterfeiting sources

With globalization of trading, pharmaceutical import licenses are multiplying. In a recent anti-counterfeiting congress held in Geneva in January 2007, a Pfizer representative mentioned that in the US there were 6,000 import licenses registered in 2006 compared to 100 in 2000. This general trend is observed in many developed countries. Therefore certifying every single supply source is a nightmare. This is certainly one explanation of how fake medicine can be found even in well organized distribution chains. An innocent parallel trader can be deceived and thereby endanger almost any supply chain. Another plague is the reimportation of low cost or donated medicines to developing countries, which reappear in developed countries with new packaging sold at a much higher conventional price[1].

This shows evidence that fraudulent business is due to the activities of a well-organized international crime industry with sophisticated manufacturing facilities and parallel distribution channels.

How to differentiate authentic and authorized products from fake or illegally imported ones?

The examples above show that marking secondary packaging with visible security features or visible coding is not sufficiently protection against counterfeiting or illegal reimportation. Many seizures have also shown that mixing genuine drugs with fake ones in a genuine reprocessed secondary box is a common way to increase illicit profits for the crime industry.

ROLAND MEYLAN co-founded AlpVision in 2001 and currently serves the company as its Corporate Communications Manager
email: roland.meylan@alpvision.com

A hope was placed in the RFID technology (Radio Frequency Identification) which consists of including a passive antenna in the packaging. But RFID technology was primarily developed for optimizing the supply chain for just-in-time delivery and not for anti-counterfeiting purposes. Therefore as for all visible features such as holograms or two dimensional bar codes, it is possible either to eradicate or fake them.

More sophisticated techniques can be found in the field of covered security elements, that is, features not visible to the naked eye and requiring dedicated detection means. The most popular solution is invisible ink, such as UV ink (visible under ultra violet light) or IR ink (visible under infrared light). To authenticate these inks, a lamp emitting light in the required wavelength range is sufficient. The drawback of these inks is that they can be bought very easily on the market by anyone. There are other chemical tracers or ink additives providing counterfeiting security, such as DNA or magnetic tracers. The problem with such special inks or ink additives is the related logistics and manufacturing procedures, such as press cleaning, temperature and pressure sensitivity, as well as interaction with other chemicals. Although very efficient and effective, their implementation and deployment are quite costly. Authentication on the fly, in the retail space for example, is also difficult.

The advantage of a covered element is that counterfeiters must know there is a security element before they can attack it. If the feature is visible, the point of attack is evident.

It is also important to note that if a security element requires a specific, dedicated detection system in the hands of the controller, then this is a clear security threat since it facilitates counterfeiting due to reverse engineering methods.

The digital image processing breakthrough

As in other industries, the digital revolution opens exciting new possibilities. Digital technologies can now

be used to fight counterfeiting and to track and trace pharmaceutical products. These digital technologies are breakthroughs compared to former "analog" ones. Instead of being issued by chemical or biology experts, they are developed by software engineers and digital imaging scientists.

The more promising new solutions are based on the same digital imaging technologies and cryptography used to protect bank notes and to secure online banking services.

A recent paper published in the *Washington Post* (October 2005)[2] mentioned that some manufacturers of home and office printers delivered printing equipment in such a way that it added invisible marks on each printed page. This of course happened without informing the users. The purpose of this hidden marking is to identify the printer when used in fraudulent printing matters. Aside from the political or legal implications, this incident shows that with today's technologies and equipment it is possible to print invisible information with normal ink and standard printing machines.

Translated into the packaging industry and security printing domain the incident described above has two important implications. First, an industrial packaging printer could produce secured packaging for manufacturers using standard printing machines and standard ink. Second, a product manufacturer can secure its products without informing the printer that the packaging contains an invisible security feature. This reduces the number of parties involved in a product security process and creates a distinct advantage because secrecy and privacy are the two pillars of an efficient security policy.

To illustrate the process of producing invisible patterns with visible ink, **Figure 1** shows the visibility of printed dots as a function of the dot size and the color used. Considering as well the nature of the paper, which always contains imperfections such as wood particles or other substances, the very small printed dots are not visible to the naked eye. And they are not identifiable with magnifying equipment because they are camouflaged in the imperfections of the paper.

Depending on the application, the printing process, the carton colour and the ink colour, the dots vary in size from about 10µm to 80µm. It is important to note that the security is also a function of the dot colour and the dot size. Security levels increase as lower contrasts are used and as the dots get smaller. Any printed surface can be protected this way, carton for folding boxes or aluminium or polymer for blister foils.

The Cryptoglyph technology

A technology has been recently developed and commercialized by AlpVision SA, a Swiss supplier of digital security printing solutions, under the name of Cryptoglyph (Crypto = encryption, glyph = marks). AlpVision is a world leader in identifying signals of very low level mixed with a noisy environment, which is in other word, finding a needle in a haystack.

The Cryptoglyph patented solution combines two elements:

1. Printing of invisible micro-points over the entire surface of the primary or secondary packaging, such as the blister foil. As these dots are invisible and spread on the whole surface of the packaging, it is impossible to replicate or to erase these dots.
2. These invisible micro-points contain encrypted information, which can only be deciphered by using the encryption key. If the detection process is performed in a unique and secured place, the key is never endangered. Deciphering the information by a fraudulent party is impossible.

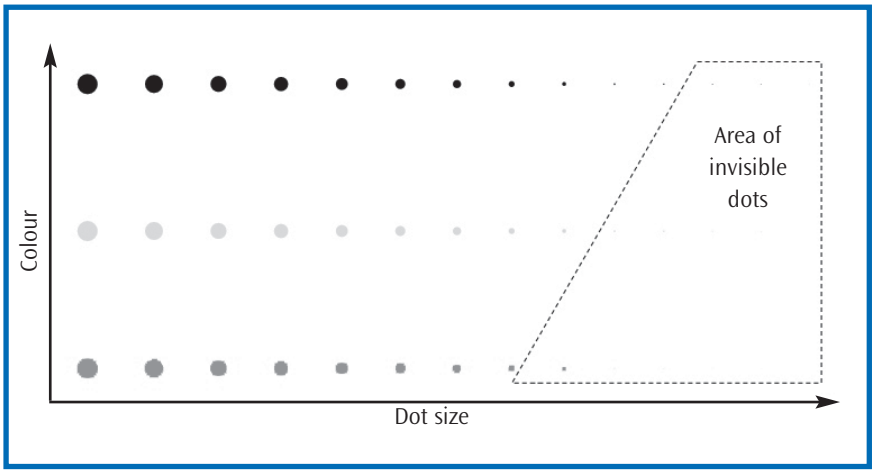


Figure 1. Area of invisible dots depending on the size and the colour of the dots as well as the printed background

These micro-points are integrated in the package design before printing and are invisible to the naked eye. They are very difficult to distinguish – even with a magnifying glass – as the dot colour and size are chosen to camouflage with the imperfections found in all printed material structures.

The detection software is based on advanced signal detection capabilities that have very low signal-to-noise ratios and built-in conceptual redundancies. The AlpVision technology surpasses other technologies, such as the 2D DataMatrix code bar because,

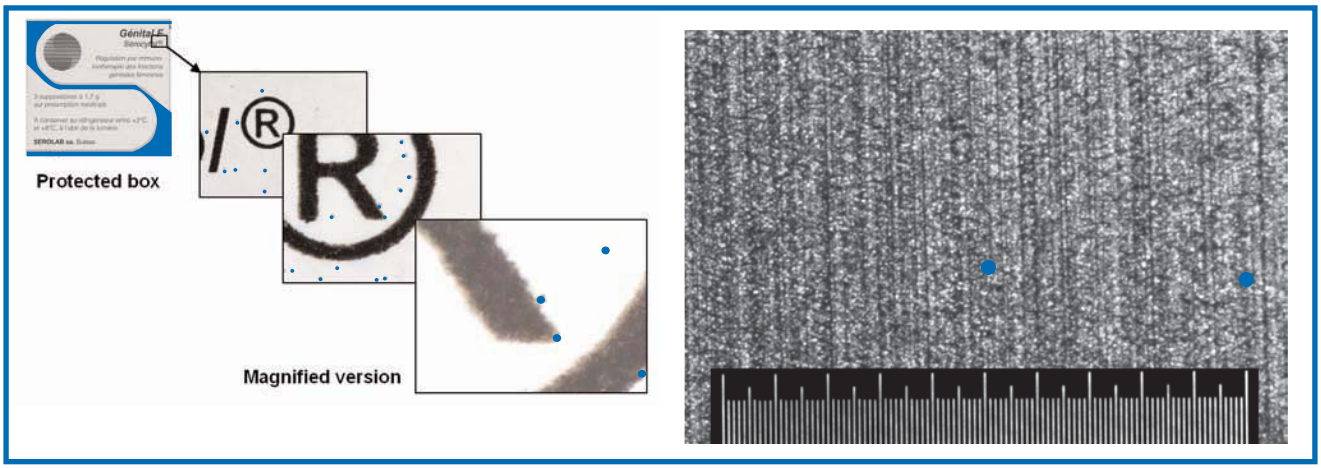


Figure 2. Left: magnified images with invisible printed dots (indicated here in blue) applied on secondary pharmaceutical packaging. Right: dots printed on aluminium blister foil (primary packaging). The whole rule represents 1mm (1000µm).

by definition, the code bar requires contrasts in visible black-and-white.

The Cryptoglyph detection process is software based and can be performed using a standard flatbed scanner or even by using a mobile phone equipped with a digital camera (camera phone). To avoid having the encryption key made available in the field, a digital image of the packaging is sent to a processing system located in a secured area, via mobile data transmission networks. Once analyzed in this safe and secured area, the result is sent back to the field controller via SMS or another modern communications means. This two-way communication process ensures the full security of the encryption system and allows instant consolidation of the field track and trace verification tests.

When comparing "analog" processes using additional security elements or visible printed codes with the "digital" ones using invisible printed dots, we see the very big difference in cost /efficiency ratios. This also takes into account the cost of the detection process.

Conclusion

Cryptoglyph is the only technology in the world providing an invisible marking with visible ink on standard printers (offset, rotogravure, digital printing, etc.). This technology requires no change in the packaging graphic layout. It is easily integrated into any current industrial printing process, without any modification.

Detection process is based on software licenses and only involves standard electronic equipment that are available everywhere.

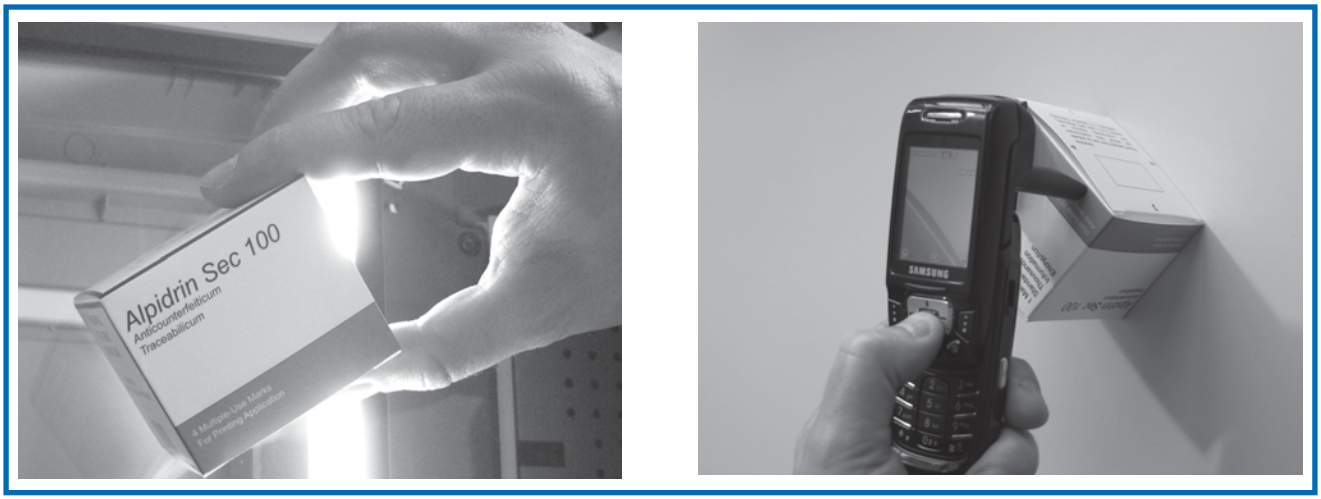


Figure 3. Left: authentication performed with a standard flatbed scanner. Right: authentication performed with a Camera Phone equipped with a lens distance adapter

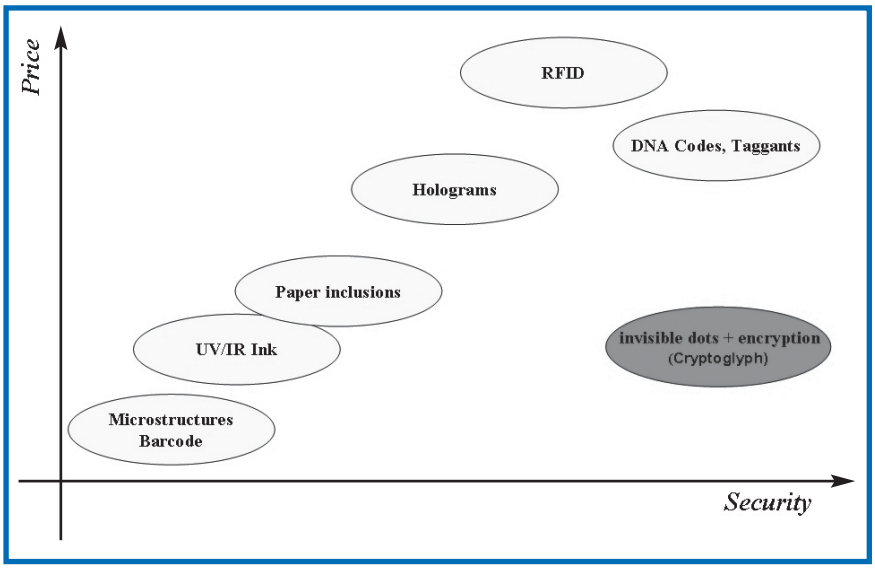


Figure 4. Performance comparison between various security techniques.

A number of industrial printers active in pharmaceutical packaging production have already added Cryptoglyph to their security processes.

Today hundreds of millions of products are protected without the consumer's knowledge by AlpVision digital security technology. The increase in counterfeit drugs or in re-importing discounted drugs involves less risk and is more lucrative compared to other criminal activities. This well organized criminal activity presents real challenges for the pharmaceutical industry. Manufacturers and legal authorities will have to cooperate and define penalty processes. Manufacturers must invest in new security techniques to enable field testing and rapid and effective reaction against unfair distributors and counterfeiters.

References

1. http://www.timesonline.co.uk/article/0,,8122-1684914,00.html
2. http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html?referrer=emailarticlepg