PACKAGING

Industry-suitable Technologies to Protect Pharma Products against Counterfeiting

As clearly stated in the new European directive 2011/62/EU\(^1\) relating to medicinal products for human use, as regards the prevention of the entry into legal supply chain of falsified medicinal products, patient safety will be achieved with the combination of three components:
- verify the authenticity of the medicinal product,
- identify individual packs or batches,
- verify whether the outer packaging has been tampered with.

These new measures, which improve the protection of public health, will be adopted by member states on January 2, 2013.

Because implementing labelling, tracking and tracing systems for products will likely result in additional costs to the pharmaceutical industry, this paper hopes to shed light on several cost-effective product authentication processes and features, which can be easily deployed and implemented within manufacturing plants and laboratories worldwide.

Authentication and Identification
Several organisations have reported that individual product coding can be used to identify counterfeits. However, more and more experts agree that visible product codes, batch numbers and expiry dates cannot be used reliably for product authentication because they can be copied by counterfeiters\(^2\). Banknotes, for example, have been serialised for decades and are still widely counterfeited. Of course, the cost invested to secure a banknote is far greater than that of medicines. However, we believe that some lessons learned in the field of high security documents can contribute to finding solutions to counterfeit pharmaceutical products.

Visible (Overt) or Invisible to the Naked Eye (Covert) Security Features
Traditionally, pharmaceutical companies have added visible security features to their packaging to prevent counterfeiting. These include, for example, holograms, kinigrams, embossing, micro printing, moiré or special ink such as optical variable ink. However, these visible features only provide minimum security and require training for effective authentication.

Fig 1. By the same token, if a company suddenly decides to discontinue the use of visible security features, consumers might mistake a genuine product for a fake.

Today, counterfeiters have the best printing equipment and components at their disposal in order to perfectly replicate the visual aspects of a packaging, including its visible authentication features. By contrast, the use of "covert" features – security features that are invisible to the naked eye – provides a higher level of security. For example, "good" counterfeit banknotes always include a replication of the visible security features, but rarely of the invisible ones. To prevent leaks, however, covert security features should never be disclosed. These features should only be shared with a limited number of trustworthy persons of the branded manufacturing company, an approach that restricts consumer access.

Anti-counterfeiting literature also suggests that a specialised scanner or a distinctive analysis is required in order to identify covert security features, making the "genuine-or-fake" verification a costly and time-consuming process. However, as in other industries, the digital or software revolution has opened up new and exciting possibilities. For example, the Cryptoglyph\(®\) on-packaging\(^3\) (e.g. folding boxes, blister packs, labels) achieves invisible protection by using normal visible ink or varnish. Fig 2 Digital security features simply require an off-the-shelf office flatbed scanner or an iPhone 4 smartphone device to perform a "genuine-or-fake" verification. In this case, the covert feature scanner can be purchased on the consumer electronics market anywhere, while proprietary hardware is the rule when security substances, taggant or dedicated invisible optical effect are used.

Replacing security consumables with software has also had a significant impact on the cost of implementing an anti-counterfeiting programme for multi-brand companies using multiple production plants. For example, when using security consumables, it is necessary to provide the various production plants with the right quantity of security features in relation to the number of packaging...
elements to produce, plus extras for the ovens. If poorly managed, this process can result in transportation and misuse of the ovens to produce counterfeiters. The use of security features reduces the risk of counterfeiting the packaging printing equipment if special ink is used or if extra features such as hologram or taggant should be inserted in the production run. By contrast, digital security features using normal ink will not alter the printing process enough to deter this. This is an important cost-saving benefit.

**Human Sensory Perception-based or Technology-based "Genuine-or-Fake" Verification**

When selecting a security feature, it is not only important to assess the cost of purchase, implementation, global deployment and management, and resistance to replication, but also how a "genuine-or-fake" verification is performed.

In this case, the various anti-counterfeiting features can be placed into two main categories: - features which use human sensory perception; - features which are machine-readable.

When using human sensory perception-based verification (visual, tactile, oral), a person will be required to undergo adequate training to be able to distinguish a genuine security feature from a fake replication, when displayed side-by-side. By contrast, when using machine-based verification, a person will only be required to follow a step-by-step process. If properly described, the latter can be performed by anyone without any specific knowledge or training.

Some methods combine a human visual decision with a device, such as the Raman Spectroscopy analysis, which is capable of analyzing the chemical components of a tablet and comparing them with the analysis results obtained in the device. Such a device may cost dozens of thousands of dollars and require some training to properly maintain. In addition, only a few analysts are generally available within a given company at a given time, forcing the manufacturer to send the suspected tablets to a dedicated lab.

As mentioned earlier, other visual features include the form factor: packaging that is its facial appearance, display surface, size, and shape, and other printing details that counterfeiters may not have identified. A discrepancy between a genuine pack and its counterfeit therefore also be identified with the help of a detailed description, stored in and provided by an online database. But this can only uncover counterfeiters until attempts are made to remedy these discrepancies.

So an important question arises as to the cost of performing a machine-readable "genuine-or-fake" verification. Because some existing digital authentication processes use off-the-shelf office scanners or iPhone-like devices to verify the authenticity of the packs, components (folding box, blister pack or label) and because these supplies are often part of an office setting, Fig 3, performing a

![Figure 3: Medical container authentication via iPhone](image)

**Security Level and Protection against Leaks**

A recent FDA report shows that organized crime is active in counterfeit medicine, as this industry represents a very attractive and easy criminal business compared to others. The use of corruption and coercion is therefore seemingly prevalent to obtain security features or to propagate the counterfeit question then arises as to the number of people and companies that should be involved in the security chain.

In the case of software licenses, suppliers are involved in the security chain on a recurring basis, exposing the recipient company to their own risk and to the risk that people are involved in producing the software. Consequently, the less suppliers are involved in critical security elements, the less leaky.

**Web-based Secure Server**

There are two fundamental ways web servers can be used. The first approach consists of using the server as a data repository system. This method involves the distribution of anti-counterfeiting features used in a given packaging or production batch. For example, the IFM system -- Interfaz Public-Members of the World Customs Organisation -- is a secure communication tool for the exchange of information between right holders and customs administrations. By using the IFM system, field customs officers have access to the 'genuine/fake' database of imported goods for counterfeiters.

The second approach uses the server to analyse different parameters of a packaging in order to automatically assess its authenticity using a digital image captured with a regular office scanner, a digital camera, or even a smartphone device.

In this case, the server is also capable of managing the deployment of anti-counterfeiting features. Because these features are digital elements, there is no need to involve various frontline suppliers in the supply chain. As for all criminal acts, the quicker you uncover them the more you are well positioned to identify the criminal source to stop it.