Teel

Anti-Counterfeiting Features in Medical Devices

Christian Herrild
Director of Growth Strategies – Teel Plastics

Kevin Kutschenreuter
Marketing Communications Specialist – Teel Plastics

Counterfeiting Background and Market Dynamics

For the purpose of this paper, counterfeiting will be defined as creating a product that is an imitation of a branded, unique, or hard to acquire product and selling it as if it were genuine.

Counterfeiting is a prevalent problem in the medical device industry, and could constitute as much as 8% of the domestic US market. The medical device industry is a popular target for counterfeiting due to its burgeoning domestic and global market value. As of 2017 medical devices are a $156 billion domestic market and approximately 40% of the global market share. China and India are also rapidly growing markets. China, a country where much medical device counterfeiting originates, had a medical device market value of nearly $79 billion in 2018, a number expected to grow significantly in 2020. India's medical device share in 2018 was $9 billion, but is expected to exceed $14 billion by 2025. Such a valuable marketplace is a clear target for fraud.

Moreover, medical device counterfeits are difficult to immediately detect, and their lower price tag is can seem like a welcome relief in a marketplace where branded products sometimes command a substantial premium.

Medical device counterfeiting should concern manufacturers primarily for the potential for injury to patients who are treated with a cheaply made or defective counterfeit. However, it is also important to consider what an injured patient could do to a manufacturing company as the result of an unidentified counterfeit device. Manufacturers could face a lawsuit for an injury resulting from what was not even their product. There is much more at stake than just lost revenue to deceptive competitors, which in itself could be 8% or more of a company's total device sales.

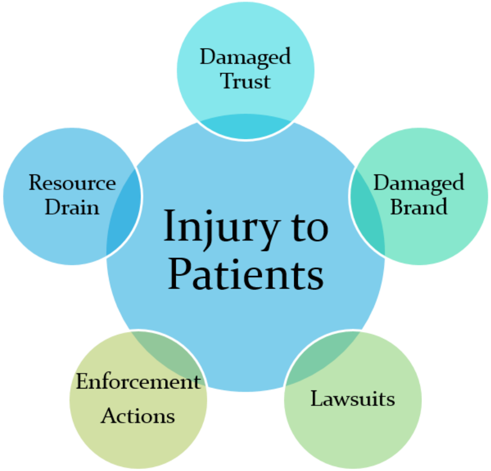


Figure 1: Potential Consequences of Counterfeiting

To help prevent these consequences, there are three types or “stages” of anti-counterfeiting measures to consider adding to your devices or packaging.

Stage one Anti-Counterfeiting

The first stage is a low-level anti-counterfeiting attempt that creates an easily identifiable marking or visual distinctiveness. This gives the purchaser assurance of a genuine product. However, this is the easiest measure of the three for counterfeiters to imitate.

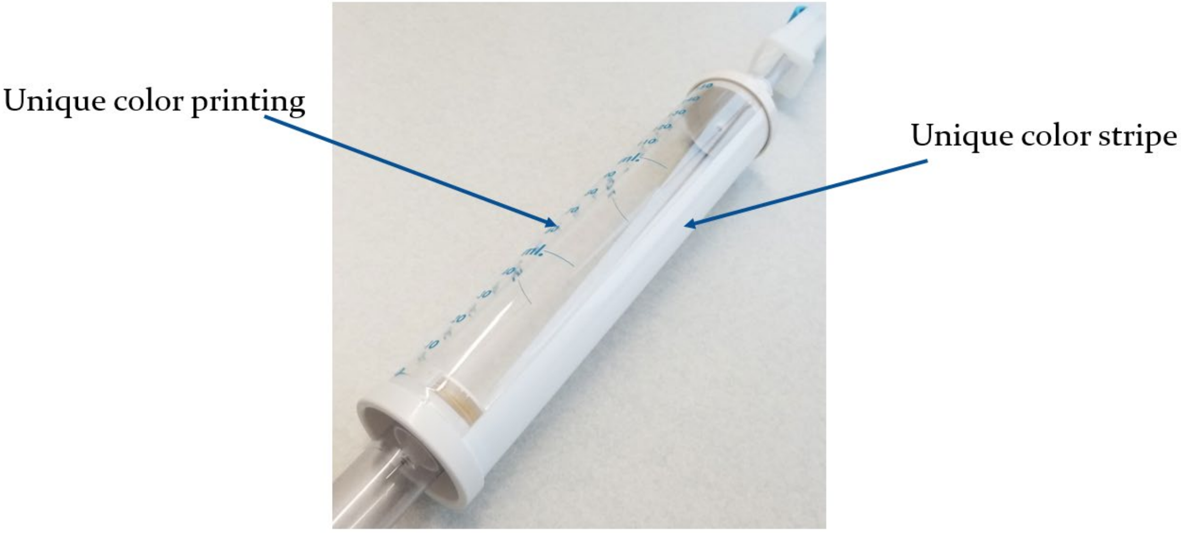
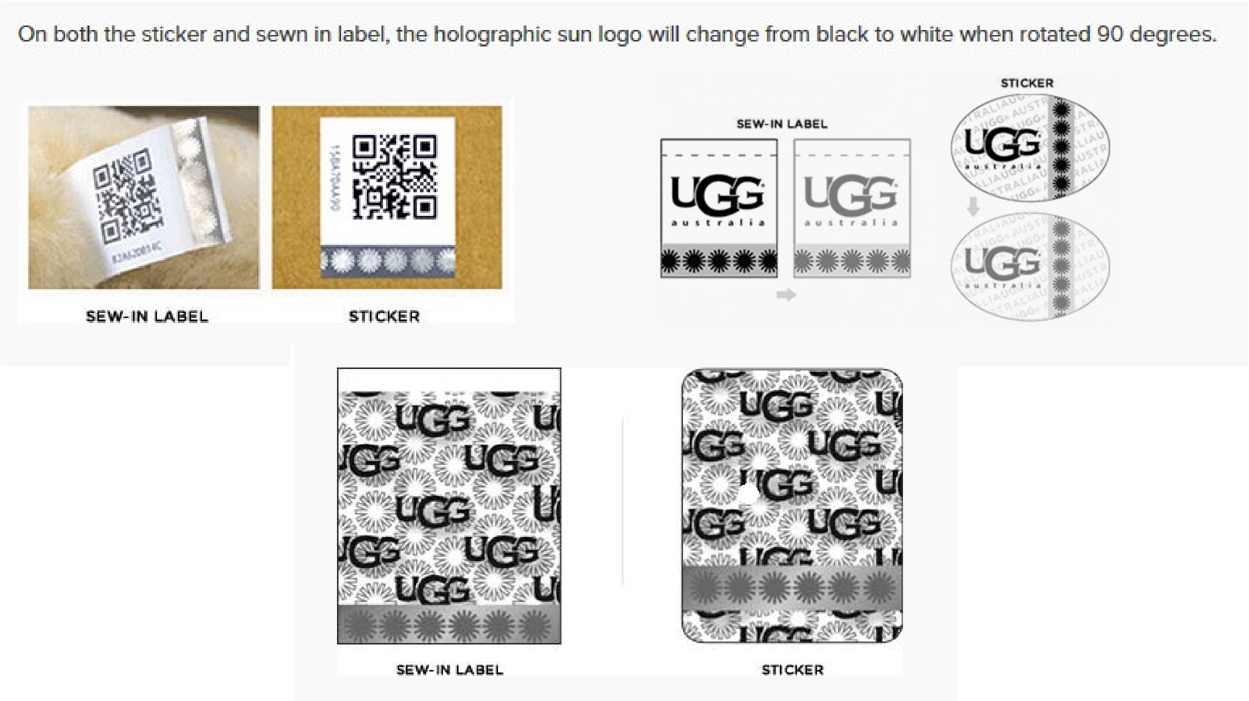


Figure 2: Unique Markings as an Anti-Counterfeiting Measure

Stage Two Anti-Counterfeiting

The second or intermediate level of anti-counterfeiting is to add a feature that, while detectable, is hard to duplicate. This includes a unique device identifier (UDI) that is not device or lot specific. These measures are meant to make the purchaser feel confident they have the genuine article, because they require more effort to duplicate on the part of the counterfeiter that stage one methods.

Ugg's products are examples of this type of measure, as they all include a sticker or sewn on label with a holographic sun logo that changes from black to white when rotated 90 degrees.



On both the sticker and sewn in label, the holographic sun logo will change from black to white when rotated 90 degrees.

Figure 3: Ugg's Product Identification Labels

Stage Three Anti-Counterfeiting

This higher level of anti-counterfeiting includes an element that is both hard to detect and hard to duplicate.

These elements can include:

- Resin taggants
- Layered printing
- Microparticles
- Fluorescence and phosphorescence

- Serialization and device identifiers

While more difficult to counterfeit, this type of measure gives no reassurance to patients that they have purchased a genuine product. In addition, the measure can still be counterfeited if the counterfeiter knows the company's system.

For example, consider the method of unique serialization and tracing as is done in the pharmaceutical supply chain through the Drug Quality and Security Act (DQSA) requirements. This allows a company to police the market for counterfeit products. However, if the company does not catch an instance of counterfeiting itself, its purchaser will certainly not be able to either by the nature of the technology.

Anti-counterfeiting Technologies

Numerous anti-counterfeiting technologies are available that fit within these different stages, and following is a discussion of some notable options. However, the discussion is not meant to be an endorsement of any of the products reviewed. It is only a technical review of what can be commercially purchased today.

Bar Code or QR Code Technologies

Bar and QR code technologies are most applicable for device packaging, but they can also be laser etched onto a device. The codes require IT infrastructure support to function, so to implement them requires committed organizational resources.

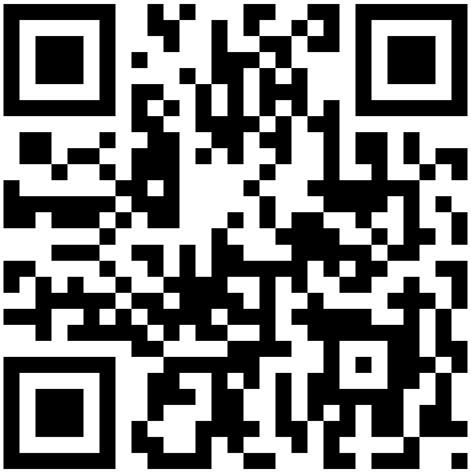


Figure 4: Example of a QR Code. This code will send you to the English Language Homepage of Wikipedia.

QR codes were originally developed for the automotive market for part tracking and tracing. One code can contain 4,296 alphanumeric characters.

Microparticles with Unique Effects

Figure 5: Microparticle Identifiers

Another anti-counterfeiting technology involves the use of microparticles. For example, Microtrace manufactures microscopic ceramic particles that emit differently colored light when illuminated with an infrared light. This involves upconverting phosphorus and an anti-stoke shift to take infrared light (heat) and make it visible light at a defined wavelength.

Layer Films and Threads

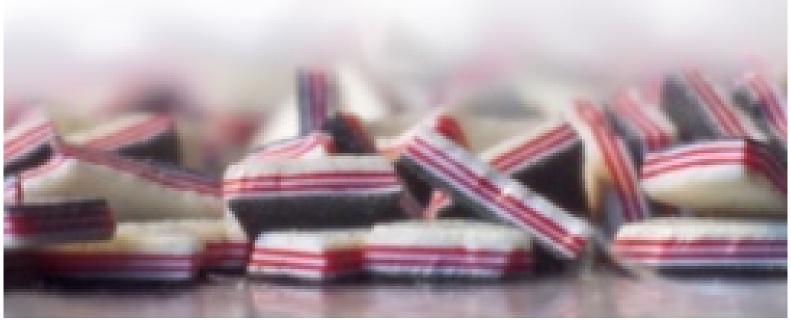


Figure 6: Color Banding Identifiers

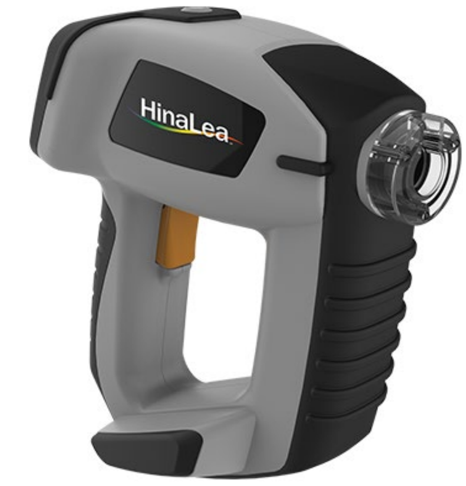
Companies like Microtrace also develop thread or films with coded color sequences. These can have other effects built into them as well, but typically, their primary feature is coded color banding. Manufacturers can rotate the banded colors for each quarter, batch, or product.

TruTag Codeable Silicon Dioxide Additives

A TruTag silicon dioxide additive technology allows manufacturers to mark items with unique information for product verification and traceability that can be instantly read and verified with a unique handheld detector. The additive serves as a marker for both medical devices and packaging. The system uses SICPA and Clariant's Plastiward technology for real-time device monitoring.

In discussing this technology, TruTag states that it has "developed codable microtags made of silicon dioxide, or silica. Silica is a material that has been affirmed as GRAS (generally recognized as safe) by the FDA and has been used as an excipient in food and medicine for decades."

Figure 7: TruTag's silicon dioxide additive



Model 4100H
Winner of SPIE 2017 Prism Awards

Figure 8: TruTag’s additive detector

SigNature DNA Coding from Applied DNA Sciences

The SigNature DNA coding system involves the application of a unique ink or coating on a product’s packaging, which is then readable with a SigNify on-site reading system.

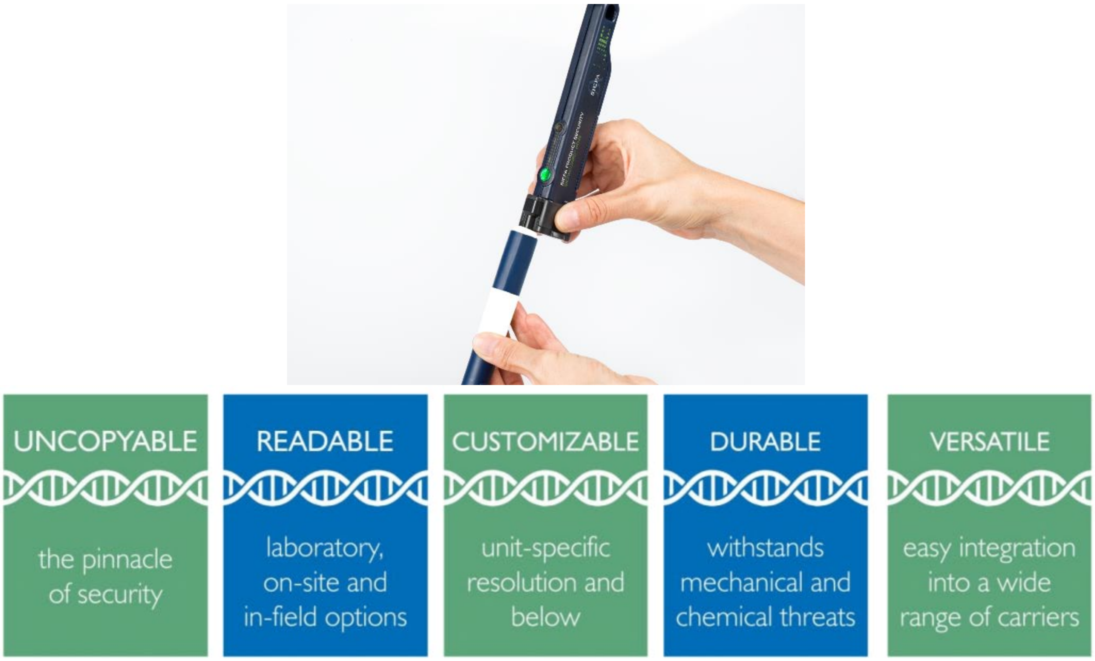

UNCOPYABLE
the pinnacle of security
READABLE
laboratory, on-site and in-field options
CUSTOMIZABLE
unit-specific resolution and below
DURABLE
withstands mechanical and chemical threats
VERSATILE
easy integration into a wide range of carriers

Figure 9: SigNature DNA System

A Technical Trend

Today, the best anti-counterfeiting systems require both a product additive of some kind and a connected infrastructure. That is, they include something in the medical device that feeds into a connected back-end IT infrastructure to allow for immediate verification. Below is a diagram of where each of the technologies discussed fits within this dual system.

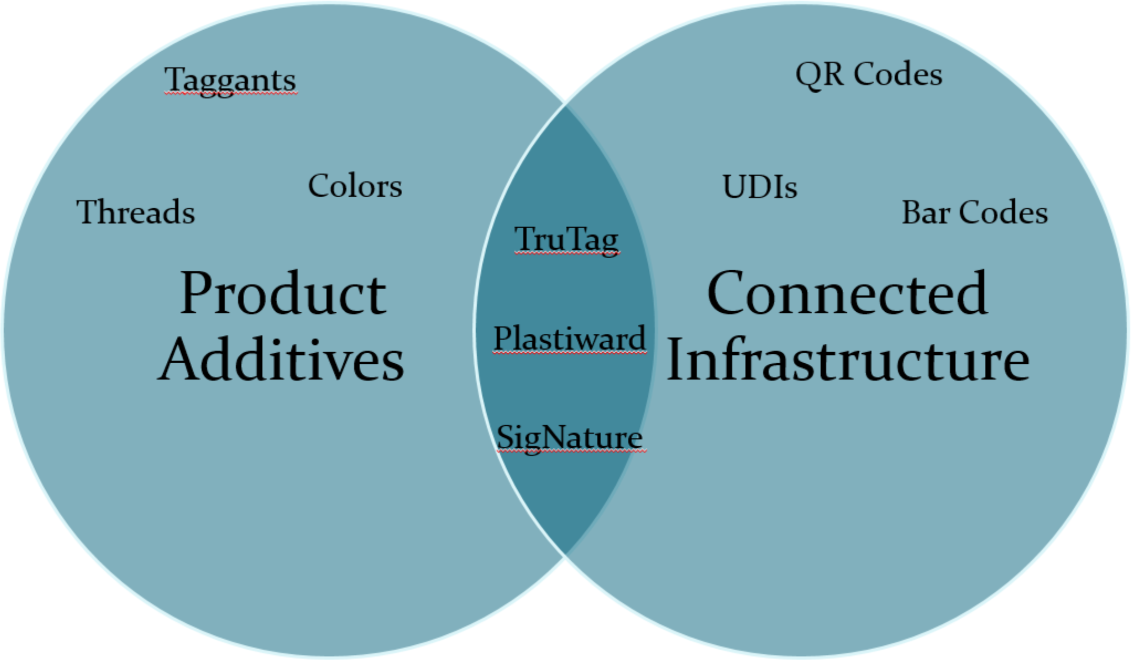


Figure 10: The Function of Various Anti-Counterfeiting Technologies

Points for Device OEMs to Consider

A number of factors will impact which of the above technologies it makes sense to implement. These include the following.

Risk Profile

In considering what anti-counterfeiting technology to use, the first question to ask is “what is the risk profile of my supply chain?” The risk is less if it is primarily based in a country like the US as opposed to China, where much counterfeiting originates.

The second question to ask is, “what is the risk profile of my device?” A higher margin device increases risk. In addition, durable goods are less liable to counterfeiting than consumables.

Use Risk

Medical device manufacturers should also consider the use risk of their devices. The higher the risk, the more important it is to ensure you have anti-counterfeiting measures in place. Consider the following questions:

1. What is the risk to a patient when a counterfeit device is used?
    - Is the device critical to sustaining life?
    - Is this a convenience use product?

2. What is the risk to your company when a counterfeit device is used?
    - How visible is failure?
    - How likely is failure to be directly attributed to a device?

Regulatory Issues

Remember that not all technologies are compatible with all device applications. More body contact means more limited options. Changes to your device in implementing an anti-counterfeiting measure may require a 510(k) or CE marking or both.

Cost

Of course, cost is always a critical issue to consider as well. More sophisticated technologies are generally more expensive and require more infrastructure to support. Starting down the road with these technologies will require an annual maintenance spend.

Conclusion

Medical device manufacturers can start by evaluating the risk in their supply chain and “chain of care”. Second, consider the goals of your anti-counterfeiting strategy and consult with experts for your application. Last, evaluate the regulatory impact of any needed changes to your product.

For more information, please contact Christian Herrild.