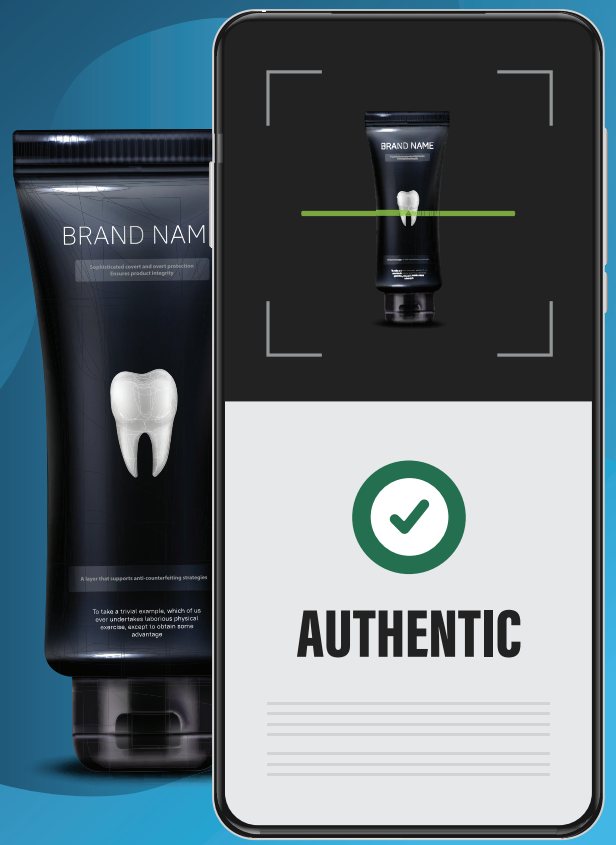
DIGIMARC INSIGHTS GUIDE

Brand Protection for Digital-First Enterprises

Digital Watermarking to Combat Counterfeiting & Promote Digital Transformation

DIGIMARC



Sobering Data, Promising Developments

In a time of significant disruptions, competition is changing dramatically. Digital transformation will separate winners from losers, making them more agile and resilient.

Digital transformation is a company-wide change in how an organization delivers value to its customers. It means bold and radical rethinking about technology, data, process, and culture. It enables companies to adapt with change, while making change a core competency of its enterprise.

Digital transformation is inevitable, while transforming the world of work. Businesses that wait will find it difficult to compete.

Becoming a digital-first company, making the crucial transformation, is often understood in terms of initiatives, such as using and interpreting data more effectively, making data more transparent, removing friction from the buying process and introducing greater efficiencies up and down the value chain. All of this is true, of course, but it fails to include a more subtle, yet in many ways, more pressing challenge—protecting your consumers and your brand from counterfeiters.

Going digital, which is having the ability to generate a digital identity for any media asset in your arsenal (everything from product images to case packs), can help with all the aforementioned benefits of digitization, while also helping you protect your brand from counterfeiters.

Growing Global Concern

There is no downplaying the threat to consumer brands today when it comes to counterfeiting. It is real and it promises to get even more challenging.

The International Chamber of Commerce estimates the cost of counterfeit and pirated goods will exceed $1.9 trillion globally by 2022.

The Organisation for Economic Cooperation and Development reports that counterfeit products are now a fixture in the world economy, representing 3.3% of global trade and 6.8% of EU imports.

But the silver lining here is that brands themselves have stepped up to push back on this challenge, and ensure consumers remain as safe as possible. By 2024, it is expected that the global anti-counterfeiting packaging market will top $4 billion, according to the consulting firm Smithers.

And beyond just packaging itself, the entire brand protection market is expected to rise significantly: by 2028, the overall market is expected to reach $1.5 - 1.7 billion[1] in critical markets, such as the pharmaceutical, automotive and tobacco industries.

Philip Morris International (PMI) has taken its own steps by founding *PMI IMPACT*, a $100 million funding initiative to "support public, private, and nongovernmental organizations to develop and implement projects against illegal trade and related crimes."

By 2024, it is expected that the global anti-counterfeiting packaging market will top $4 billion

Broad Attack on Brand Identity

Many consumers, when they think of counterfeiting, often think of fake luxury items, knock-off designer bags or watches in street markets, but the challenge is multifaceted and far more complex. It involves challenges across a wide spectrum of brand assets, affecting intellectual property, packaging, products, brand reputation, as well as the safety and health of consumers.

And when we talk about these attacks, it is not just an issue of fake products. Consumer brands must also contend with so-called "grey goods," which are authentic products illegally diverted from the supply chain (i.e., manufactured off the books). Related to this problem, but unique in its own way, is product diversion, which is when an item is moved out of authentic markets and either sold in other unauthorized markets unknowingly, or re-entered into original markets to evade taxes.

Serialized identities on packaging and traceability can help with product diversion; brands can track the product through the supply chain and analyze normal versus suspicious location data.

1. Counterfeit Selling Online

There are now a number of platforms and vehicles on which counterfeit sellers can connect directly with consumers. And while some consumers knowingly buy fakes, many others believe they are buying an authentic brand product, and become unwitting accomplices. But regardless of the reason, the impact is significant.

One of the ways counterfeiters entice consumers, is by stealing authentic brand images and using them as a "front" for their fake goods.

There are number of venues where fake products are sold, but a few of the main offenders are:

- **Rogue Websites/Cybersquatting** – Counterfeiters create legitimate-looking, faux-branded websites to confuse consumers and sell them knockoff goods.
- **Mainstream Marketplaces (Amazon, Etsy, eBay, Instagram)** – The marketplaces do not sanction counterfeiting—and have begun to police their platforms more aggressively—but the ease of "setting up shop" makes them inviting to criminals.
- **Image-Based Sites** – Some counterfeit websites avoid HTML copy (text) altogether, instead relying solely on images, making them much harder to detect through traditional web crawlers.

2. Altered Packaging and Product Labels

"Doctored" packaging knockoffs, of an obvious poor quality, used to be an easy indicator of a fake or unreported product. When the package had a spelling error or a poorly reproduced logo, this was a clear signal of malfeasance. But now with design software readily available, the days of shoddy packaging design are over.

According to a recent *New York Times article*, "Even if it's not absolutely identical, fake packaging can be pretty convincing since design technology makes it so easy to match and reproduce fonts. And without the real package to compare, it's hard to be sure."

A *Los Angeles Times article* detailed the sophistication of counterfeiters and how their graphic design talents, in particular, are endangering public health in California, as counterfeiters produce fake cannabis vapes: "The phony packaging is convincing to the untrained eye, some even carrying bogus labels that appear to carry state-required test results."

3. Infringement of Intellectual Property

Copyright infringement is another worrying, and evergreen threat to brands. According to the U.S. Copyright Office, "copyright infringement occurs when a copyrighted work is reproduced, distributed, performed, publicly displayed, or made into a derivative work without the permission of the copyright owner." This can take many forms, but using brand images without permission is a prominent example.

Other attacks include individuals or organizations that register your trademark in countries where counterfeit production and trade are commonplace—known as trademark squatting—which can be costly and cause problems if you try to do business in those countries.

Loss of Life, Health and Revenue

For customs officials, government regulators, consumers goods companies and families who've been affected by counterfeit goods, the impact of this problem is immeasurable. **The challenges include:**

Human Loss of Life Due to Counterfeits

Human Injury Due to Counterfeits

Human Sickness Due to Counterfeits

Increased Revenue Loss Due to Product Diversion

Increased Litigation Due to Product Fraud

Required Compliance with Government Initiatives

Industry Pain Points – Three Examples

1. PHARMACEUTICAL

The World Health Organization (WHO) has estimated that 10% of global pharmaceutical commerce, the equivalent of $21 billion worth, involves counterfeit drugs. The results of this proliferation, of course, can be deadly.

It is estimated that between 60,000 and 80,000 children in Niger with a fatal form of malaria were treated with a counterfeit vaccine. The fake vaccine contained only chloramphenicol, an antibiotic that is safe when it combined with another vaccine. It is estimated that approximately 100 children died from the incident.[1-2]

The Centers for Disease Control (CDC) is so concerned about the issue of counterfeits, it advises American citizens to avoid buying medicines overseas. On its website it notes, that while 1% of medicines in the U.S. are believed to be counterfeit, "studies show about 9%-41% of medicines sold in low- and middle-income countries are counterfeit."

Pharmaceutical companies must contend with a host of complex and interrelated challenges, including:

- Protecting their consumers health as well as their brand's reputation
- Identifying size/scope of counterfeits in a given market
- Changing packaging designs to foil counterfeiters
- Meeting the legal requirements of the European Commission's Falsified Medicines Directive
- Managing multiple anti-counterfeit methodologies and integrate new technology with each one
- Educating supply chain stakeholders on how to identify fakes versus authentic products

Industry Pain Points

2. TOBACCO

In India, one out of every *three cigarettes is fake*. It's an astounding fact and helps frame up the challenge of counterfeit tobacco products, particularly in the developing world.

As a result, the Authentication Solutions Providers' Association (ASPA) in India has issued an advisory report urging the government to eliminate illicit tobacco trade in the country, following requirements issued by the WHO's Framework Convention on Tobacco Control.

According to a 2019 report by the Indian government, "Causes & Control of Illicit Tobacco," there is a "98% correlation between the levels of taxation and retail prices, which impacts the affordability of cigarettes." And because some consumers want to avoid these taxes, they purchase contraband cigarettes, which evade taxes and duties while exploiting arbitrage through illicit trade.

Along with the obvious concerns of preserving the safety of their consumers and preserve their brand's good name, tobacco manufacturers face the challenges of:

- How to accurately identify the size and scope of problem
- Issue of suppliers and retailers participating in counterfeiting in emerging markets, difficult to remove counterfeits
- Needing multiple brand protection technology to work together seamlessly
- Need to teach consumers how to identify safe items
- Understand regulation requirements and barriers

Industry Pain Points

3. AUTOMOTIVE

The Toyota Corporation estimates that, if you accounted for every single Toyota vehicle part (even screws), there are over approximately 30,000 parts. If you picture the dozens and dozens of different suppliers making individual items, say airbags or brake pads, you begin to appreciate the near limitless opportunities for enterprising counterfeiters.

The European Office of Intellectual Property (EUIPO) estimates that €2.2 billion is lost every year by the legitimate parts industry to counterfeit tire sales, for example, and €180 million each year due to counterfeit battery sales.

A 2019 article in the *World Trademark Review* documents this acute threat to driver safety by highlighting some of the main components targeted by criminals:

- **Airbags** – Counterfeits do not comply with the exacting specifications designed to prevent physical trauma
- **Engine & Drivetrain Components** – Knockoffs contribute to engine failure and pose a fire risk
- **Brake Pads** – Fake versions can be made of sawdust and compressed grass or asbestos, which impacts stopping ability
- **Electrical Components** – A threat of electrical failure and fire risk
- **Wheels** – Counterfeit parts quickly become compromised by normal wear
- **Fake Windscreens** – May shatter easily, showering passengers with glass fragments

Along with absolute necessity of protecting the safety of their consumers, the automotive industry is focused on a number of issues, including:

- Expensive litigation and settlements due to loss of life or injury
- Making anticounterfeit methods difficult to copy
- Identifying the location of counterfeit creation
- Helping consumers identify which products are safe
- Developing corrugate packaging that makes customs communication and shopping efficiencies easier

Digital Watermarking: The Indispensable Defense Layer

Product packaging stands at the very heart of the modern supply chain, and because of this critical role, it is inevitably a key target for counterfeiters bent on defrauding consumers, and in doing so, potentially harming their safety as well.

Defending your products and packaging requires a multilayered approach, which can include the use of covert features to enable multi-layer- to dual-authentication processes. And when these processes are combined with overt markers, such as RFID tags or holographic stickers, they can provide a complex defense against tampering. Digital watermarks, specifically, can be used alone or in conjunction with other forms of brand protection solutions and/or software.

Digital watermarking provides a crucial layer in this defense, because it is a digital identifier that can function both in a covert and an overt capacity.

In a covert use case, Digimarc Watermarks can serve as an imperceptible and unique data carrier repeating many times across the product, packaging or labels, to create a redundancy that results in more reliable, efficient identification.

In addition, Digimarc Watermarks have item-level identities that can be serialized to provide unique references for each product.

Digital watermarks can be used alone or in conjunction with other forms of brand protection solutions and/or software

Three Key Methods for Effectively Utilizing Watermarking

Deception is a key weapon in the counterfeiter's arsenal, but deception is equally important to anti-counterfeiting tactics. Consumer brands that can effectively use deception can regain security for their products and their consumers. Digital watermarks can be employed in a number of ways, depending on the product, industry, media, or object to be enhanced, and the level of the threat.

1. Security Features

Security is paramount when it comes to protecting your brand from the nefarious tactics of bad actors. The strategic use of digital watermarks as a security feature can help brands confront, not only counterfeiting, but also product diversion and the gray market as well as the issue of untrusted suppliers making overruns or farming out component work.

Security with packaging is achieved through obscurity. The key is to use a variety of different security features, including Human Readable, Overt, Covert and Confidential (a variant of Covert). The goal is to create expense/heterogeneity and drive the counterfeiter elsewhere.

You can think of them as security levels, which provide a formidable defense:

1. **Human Readable** – This is simply a printed symbol or mark that is obviously some kind of security feature. No deception, just a clear warning that the media is protected.
2. **Overt** – This is adding machine readable marks, such as a hologram or visible digital watermarks (as a series of dots, for example) on a printed label.
3. **Covert** – Imperceptible digital watermarks such as Digimarc Watermarks, used on packaging, for example, in combination with overt marks or security inks.
4. **Confidential** – Proprietary security features created in a tightly controlled manner for high-value items. As the name suggests, these are confidential methods that neither the brand protection provider or the customer would ever reveal.

2. Granularity of Identity

Adding unique, serialized digital watermarks on product packaging communicates information at the batch, lot and item level, helping brand leaders to know when the products were produced and distributed. This granularity allows the implementation of a number of use cases, including traceability and supply-chain monitoring, as well as for the ability to understand sources of product leakage for product diversion issues.

Digimarc Watermarks can be provided at any level of granularity and is a function of the granularity of the identifier (number) used in the symbology and the workflow/supply-chain in which it is used. The levels are:

1. **SKU** – Object class granularity with, for example, a cereal box, where all the variants with different graphic elements still have the same GTIN.
2. **Lot** – The object class is segmented into lots or batch as a function of production and supply-chain.
3. **Date** – The object class, plus the date, is used to inform workflows and as a mechanism to narrow the product identity by sell-by date, for example.
4. **Instance** – Each instance of an object has a unique identifier.

3. Obfuscation

Complexity is the enemy of the counterfeiter, and covert digital watermarks help brands when dealing with complex situations, such as:

- Being the target of sophisticated or state sponsored counterfeiting.
- Working with unscrupulous suppliers (making overruns, farming out component work, etc.)
- Securing legislated workflows, such as tax stamps for alcohol and tobacco products.

The covert nature Digimarc Watermarks enable the entire surface of the object to be used to create complex and interconnected enhancement strategies. Digimarc Watermarks can be combined with services that can harden and secure against reverse engineering.

Depending on the level of the threat, consumer brands can choose one of several strategic levels:

1. **None** – No attempt to create artificial complexity; only add digital watermarks.
2. **Simple** – Interconnected identifiers or signaling.
3. **Advanced** – Interconnected identifiers combined with software components for security constructs.
4. **Complex** – Extensive use of obfuscation and secure loading of software components and artwork binding.

"Consumers may find it difficult to distinguish a fake from a legitimate automotive part by simply looking at the outer appearance. Consequently, consumers inadvertently purchase products that could be sub-standard and unsafe. There is always a risk of underperformance when a counterfeit product is used, as counterfeit goods differ dramatically in quality."

– Sophie Pereson, World Trademark Review, May 2019

Deploying Digital Watermarks for Business Success

A brand that employs a complex set of security and obfuscation features to protect their products and their consumer has taken a key step forward. Think of brand protection as applying a series of interconnected locks around the product. The more locks, and the more tightly they are strung together, the stronger the security.

The example below is an excellent illustration of how, using a package of pharmaceuticals as an example, brands can ensure the security of their products by using Digimarc Watermarks, in conjunction with other identifiers and inks, to ensure the product can easily be identified as authentic, despite a series of attacks targeting multiple areas.

Product	Product Package	Case Pack	Corrugate Shipping Container
1 Laser etched direct part marking	2 Overt code	4 Overt code	6 Overt batch/lot
	3 Covert code	5 Covert code	7 Covert serialized

"WestRock is developing a network of new technologies and partners enabling packaging solutions that will support brand authentication throughout the supply chain and reduce friction for the global movement of goods."

– John Dwyer, Vice President, Business Development & Enterprise Solutions

WestRock

Going Digital, Getting Protected

'Going digital' means many things to many people, but at the end of the day, as *McKinsey & Company* writes, it is "a way of doing things," creating value and "building foundational capabilities that support the entire business." And there is no greater value than one's brand, its good name, and the trust consumers have in that good name.

When you add Digimarc Watermarks to packaging, labels, case packs, product images, and even directly on the product themselves, you not only are going digital—providing media with a unique digital identity—but you are also standing up for your brand, and most importantly, putting your consumer's health and safety first.

Decades of Anticounterfeiting Expertise

Only Digimarc offers a robust brand protection solution to help companies implement a layered approach to protecting their physical and digital assets. This singular expertise is based on decades of innovation and experience, beginning with Digimarc's founding in 1997, and growing in the ensuing years working with governments to deter counterfeiting and detect tampering on banknotes, driver licenses and other government-issued documents.

Digimarc's brand protection applications support a layered approach to safety:

Product & Package Identification

Leveraging Digimarc Watermarks for use on products and packaging makes it easy to authenticate an item. Authentication occurs by scanning a Digimarc-enhanced item with a mobile app, web-based scanning, inspection system camera or other handheld systems enabled with Digimarc detection software.

Supply Chain Authentication

Secondary and tertiary packaging can easily be authenticated and accelerated through the supply chain and customs.

Digital Images & Documents Authentication

Digimarc is easily added to digital images and documents to quickly identify the authenticity and rightful ownership of digital assets used across online ecosystems.

Get started today by visiting digimarc.com/brands

Digimarc Corporation
9405 SW Gemini Drive
Beaverton, OR 97008
T: +1 800 DIGIMARC (344 4627)
F: +1 503 469 4777
info@digimarc.com
www.digimarc.com

Digimarc Corporation (NASDAQ: DMRC) is a pioneer and leader in digital watermarking solutions and the automatic identification of media, including packaging, commercial print, digital images, audio and video. Digimarc helps customers drive efficiency, accuracy and security across physical and digital supply chains. Learn more at www.digimarc.com.

[1] The Insight Partners (2021). Global Authentication and Brand Protection Market to 2028. p. 51. c
[2] en Ham M. Health risks of counterfeit pharmaceuticals. Drug Saf. 2003;26(14):991-997.
[3] ten Ham M. Counterfeit drugs: implications for health. Adverse Drug React Toxicol Rev . 1992;11(1):59-65.