Protect Your Brand, Power Your Success



How to fight counterfeiting and the assault on brand identity

The attacks on your brand have never been more numerous or costly. From counterfeit selling online to IP theft, now is the time to create a sophisticated defense strategy. Find out what the challenges are and how you can arm your organization with anti-counterfeiting and brand protection tools that work.



The Challenge for Brands: By the Numbers

Explosion of Online Brand Images

When Google Images began in 2001, it launched with 250 million indexed images. The most current stats available from Google are from nine years ago (2010), when that total had leaped to 10 billion images.

One can only imagine what that astronomical figure is today.

For ordinary users of Google search, this is an unparalleled, singular resource. For brands, it's a management challenge as they try to document, identify and manage their new and old assets across the web. And for counterfeiters—looking to sell fake brand items to both suspecting and unsuspecting consumers—it's a treasure trove to support nefarious practices.

Counterfeit products today are a massive business, causing trillions in lost sales for brands. The 2018 Global Brand Counterfeiting Report estimated that losses suffered due to global counterfeiting in 2017 was \$1.2 trillion. This includes all outlets, including vendors selling fake brands at flea markets and counterfeits sold on Amazon.

And the online portion of this criminal activity alone is devastating: costing brands \$323 billion in 2017.

The Instagram Case Study

Instagram is now an important sales channel for many brands. Brands will typically use a separate set of social images for social promotion, as opposed to the standard product images they use on their websites or online marketplaces, such as Amazon. Because brands are so active on social channels, they're increasingly becoming targets for counterfeiters. A 2019 study from analytics firm Ghost Data identified approximately 56,000 counterfeit accounts on the platform, and this represented a 171% increase compared to three years earlier.

More than 64 million posts and an average of over 1.6 million Instagram stories per month saw a growth of more than 341% compared to three years ago.

NBC News covered the Ghost Data study and reported "the researchers can't necessarily tell real from fake by just looking at the photos of the products, with some high-quality counterfeits almost indistinguishable by photos or videos."

In a nutshell, this is the core of the problem. Not even expert eyes can decipher what's what.

There are two overarching principles to remember when considering the problem of counterfeits:

- While brands often use separate, social-only assets on their channels, counterfeiters often use authentic product images to sell knockoffs and diverted products online, underscoring the need to protect product images.
- Misuse of authentic product images can serve as a clear signal of possible counterfeiting activity.



Brands that are looking for a more airtight approach to protecting their images on social media platforms, should consider digitally watermarking both their product images and the images they've reserved for social usage (see "Protect Brand Assets" on page 6 for more information on digital watermarking).

Brands Under Assault

War on Multiple Fronts

Consumer brands and their products are under attack today from a variety of actors and from a variety of directions. And while counterfeiting is the most prominent and the most costly aspect of this brand assault, there are a number of fronts that are forcing brands to think more about brand protection.

The IP Battles

Copyright infringement is quite common and an 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.

Intellectual property and trademark laws vary by country, but copyright laws are more globalized and can be used quickly and efficiently to address misuse of product images.

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. Therefore, registering your trademarks globally is an important tool to combat that tactic. Then there is the issue of patent stealing, which takes many forms, but can include instances when a company knowingly begins using your IP without paying a license. In essence, they are making a calculated risk: if they are sued in court for IP infringement by your lawyers, the financial restitution may be acceptable to them. They choose to take the hit.



Counterfeit Selling Online

Along with IP battles and the old-school street markets where counterfeit goods are sold face-to-face, there remains the complex, rapidly changing world of selling counterfeit goods online. There are now a number of platforms and vehicles on which counterfeit sellers can connect directly with consumers. It's important to point out that some consumers knowingly buy fakes, while others believe they are buying an authentic brand product. It's not easy to generalize about consumer behavior.

Rogue Websites/Cybersquatting – Counterfeiters create legitimate-looking, faux-branded websites to confuse consumers and sell them knockoff goods. If it looks like a Gucci website, for example, this is half the battle of getting consumers to provide their credit card information. A 2018 report by the United States Government Accountability Office (GAO) on counterfeit

markets warned: "When selling online, counterfeiters may post pictures of authentic goods on the websites where they are selling counterfeits and may post pseudonymous reviews of their products or businesses in order to appear legitimate."

Use of Top-Level Domains – One of the most effective ways of creating legitimate-looking websites is through the use of generic top-level domains (gTLDs). Mainstream gTLDs like .com, .net and .org used to be subject to restricted use; now their availability is unrestricted. Consumers on the web still perceive sites with these gTLDs as "safe," due to prior restrictions, increasing the damage and risk when a counterfeiter obtains one to fool customers. For example, www.gucci.net certainly looks like it could be a legitimate site, but it is not.

By utilizing generic top-level domains, counterfeiters can now quickly and easily list and re-list products and images, keeping one step ahead of the brands trying to police them. Registering your trademarks and purchasing web domains across a wide variety of gTLDs and variations on brand names are important tools to block, and facilitate the removal of counterfeit web pages.

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 (web crawlers such as Google search rely on "reading" HTML text to understand what a website is about).

Mainstream Marketplaces – Online marketplaces are important and critical outlets for consumer brands, with more shoppers moving online than ever before. Yet counterfeiters are now comfortably embedded in these outlets. According to writer Roomy Khan in an 2019 *Forbes* article: "Effortless account and storefront setups at marketplaces such as Amazon, Etsy, eBay, Instagram, and others are giving the counterfeiters legitimacy and access to millions of consumers."

And while there is no suggestion these online marketplaces are sanctioning counterfeiting, the ease of "setting up shop" makes them inviting to criminals. This illegal selling can go for months and years without brands detecting the misuse—and because there is often no way to alert them a brand image is involved—this activity can go on undetected.

The 2018 GAO report on counterfeiting echoed concerns that a huge percentage of goods sold online through mainstream marketplaces by third-party vendors were counterfeit. The GAO purchased 47 brand name products from third-party sites and found that 20 were counterfeit. And while the goods were fake, it's very likely that the brand images were not fake, but authentic digital images used to "close the deal" with consumers.

Amazon is showing signs of getting tough on counterfeiters. A June 2019 article in GeekWire reports, "Amazon and Nite Ize, a Colorado-based maker of mobile accessories and LED products, filed a lawsuit...against 11 individuals and business entities across three countries, accusing them of selling counterfeit goods on the tech giant's online retail platform."



Social Media Impersonation – In the age of multi-channel marketing, every digital asset is a sales channel, and more than ever this includes social media. The counterfeiters have noticed brands are selling more products via social sites, so they've naturally begun to set up their own "branded" accounts on popular social media platforms in order to siphon "likes"—and purchases.

Real-World Consequences for Brands

A Disturbing Picture

The 2018 Global Brand Counterfeiting Report put the loss due to counterfeiting at \$1.2 trillion. And while nearly anyone can appreciate the black-and-white numbers related to lost sales, there are a number of other "soft" and "hard" costs that result from counterfeiting:

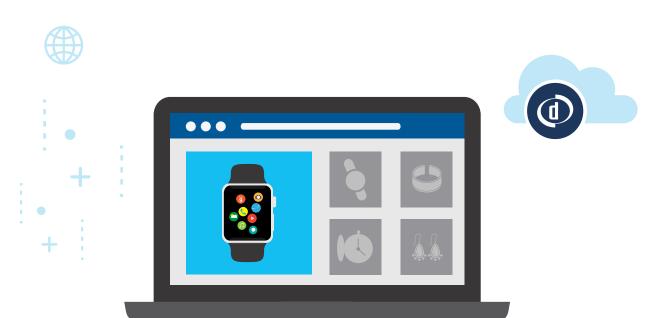
Plunging Prices – Counterfeiters don't have the expenses and overhead you have as a legitimate brand. They can sell counterfeits at a cut-rate price, which can force you to lower prices to compete against the fakes.

Reputation Hit – Here's a potential scenario: A consumer buys a counterfeit of your product. They may not know it is a fake and—when finding the quality is poor—they communicate to your company their dissatisfaction. You now have a customer who is upset with your brand—and may become even more displeased with you when they learn they've been sold a fake.

You've worked hard to establish your brand's reputation in the marketplace. Unhappy customers feeling duped, or believing your brand's quality has diminished, pose a real threat.

Damaged Partner Relationships – Partnerships are all about trust. When partners or distributors see counterfeits on a popular online marketplace for a price that is far below the price negotiated by the two of you, there can be serious friction that can weaken relationships.

Legal Fees – To stand up for your brand's rights, you'll need legal help to fight back. And whether you are using the resources of in-house legal counsel or hire an outside firm—it costs money to go after the offenders.



✓ Your Anti-Counterfeiting Strategy

Standard Practices

There is no one, single silver bullet for protecting your brand. Like many complex problems, it requires a layered approach. But there are fundamental actions you can take to curb and limit the attacks on your brand, and online counterfeiting in particular.

Digitally Watermark Brand Assets - Stolen brand images serve as a "friendly front door" for counterfeiters, who use them to legitimize their rogue websites and social media channels. Superior to visible watermarks or fingerprinting solutions, Digimarc Barcode for Digital images is repeated throughout the pixels of your images, identifying them as yours even when cropped or compressed (more on Digimarc Barcode for Digital Images below).

Get Registered — Register your trademark in every country where you may want to defend it (i.e. sell your products).

Contact Police/Government Authorities - Lobby and contact relevant government and law enforcement agencies in the countries where illegal products are manufactured and sold. Make local officials aware of how the illegal activity is hurting your business and preventing consumers, vendors and other companies in their countries from sharing in the legitimate benefits from your company and its products.

Protect Your Product – Leverage digital authentication tools to uncover unauthorized use and thwart counterfeiters. Digimarc Barcode for Digital Images helps brands manage the use of images throughout the supply chain and across the public internet, providing greater insight into where brand assets are being used to monitor licensing efforts, channel partners and potential diversion. Digimarc Barcode for packaging provides a covert way to unobtrusively add data in your package design for greater insight across the supply chain. In addition, HP Inc. features Digimarc Barcode for serialized and connected packaging that enables traceability across a product's lifecycle. With Link from HP, each individual package has a unique identifier that can be used to guard against product diversion, fraud and counterfeiting.

Boost Product Accessibility — Sell on localized e-commerce marketplace sites and/or set up your own e-commerce sites in the regions where illegal manufacturing and selling are performed. The idea here is to make your legal product more accessible, and in doing so, make it harder for consumers to choose an illegal product because "they can't find" the authentic product.



Protect Brand Assets

Manage Images & Digital Assets with Intelligence

Ensuring that brand images and other assets are protected throughout their lifecycle is essential to managing your brand and fighting back against counterfeiting. Protecting your images is an essential layer to your larger brand protection strategy.



Digimarc Barcode for Digital Images

Digimarc Barcode for Digital Images is an imperceptible code that is easy to implement and provides persistent brand protection that is superior to visible watermarks or fingerprinting solutions. It remains effective even through file compression, format changes, editing, cropping and other manipulations.

Digimarc Barcode enables brands, rights holders and digital-asset managers to better manage the use of images and other assets throughout the supply chain and across the public internet.

The Digimarc solution combines these imperceptible identifiers with complementary crawl services, customers benefit from greater insight into where brand assets are being used—providing unprecedented intelligence for better brand management. In partnership with PhishLabs, a leading surveillance company, Digimarc delivers crawling services on public websites for greater insight into how your brand appears to others.

Extend Your Reach

Digimarc customers have access to a convenient web-based dashboard delivering information about when and where Digimarc's web crawling service identifies your brand assets online. It provides actionable information to help customers oversee licensing efforts and management of retail and channel partners.

The bottom line is that your stolen images will have an imperceptible mark that enables you to prove ownership of an image with 100% confidence. The crawling service can extend your own surveillance efforts, helping you focus on where your stolen images are on the web. In many cases, this will reveal counterfeit operations.

Adobe Dynamic Media

Adobe's Maxwell Mabe writes that the mantra for brands should be surveil, detect and defend. He adds, "Let's face it: The bad guys, just like pirates seeking treasure, never stop thinking of how to capture your assets," Mabe writes. "Their survival depends on circumventing your protections, and now and then they succeed. This is why surveillance—monitoring—is so important."

Digimarc and Adobe are longtime partners, and customers of Adobe Dynamic Media, an advanced Digital Assists Management (DAM) platform, can utilize Digimarc Barcode for Digital Images within the convenience of their Dynamic Media dashboard. While many brands bifurcate social and product images, Dynamic Media makes it easy to create dozens of presets and aspect ratios so this bifurcation of images is not necessary; making it easy to watermark and protect all your assets.

Dynamic Media and Digimarc offer a proprietary method of adding Digimarc Barcode at the pixel-level of images that imperceptible to humans, but detectable to Digimarc's web crawler.



Conclusion: Protection Requires Innovation

Digitally-connected consumers and a new generation of brand- and web-savvy entrepreneurs are changing the face of brand loyalty and consumption. Social media influencers can create their own successful "brands" with millions of followers virtually overnight.

But there is no substitute for the well-earned brand equity you have established over the course of many years, if not generations, and invested everything in order to establish brand loyalty amongst your consumers. Brands with their own hard-won following have the advantage of a strong foundation—but are also ripe for disruption and diversion. Counterfeiters are black-market brand experts, and they are constantly innovating in order to siphon away your audience and your revenue. Brands must continue to innovate and establish strong, multi-layered anti-counterfeiting strategies in order to stay ahead of black-market competition.

We've outlined a list of resources to help you protect your brand and power your success.

Additional Resources:

- World Trademark Review: Alternative strategies for fighting counterfeits online
- <u>Digimarc Barcode</u> for Digital Images
- Dynamic Media Platform
- Dynamic Media Classic and Dynamic Media blog for tips and guidance
- Go to the Digimarc Lab & See How We Protect Images
- Webinar: Content Protection Strategies
- Trademark Basics from the U.S. Patent & Trademark Office
- · Harvard Business Review: 8 Ways Brands Can Fight Counterfeits in China

Sources

https://www.nbcnews.com/tech/tech-news/scammers-have-turned-instagram-showroom-luxury-counterfeits-n997256

https://techcrunch.com/2010/07/20/google-image-search/

https://www.gao.gov/assets/690/689713.pdf

https://www.businesswire.com/news/home/20171222005383/en/Global-Brand-Counterfeiting-Report-2018-Counterfeited-Goods-Counterfeiting-Report-2018-Counterfei

https://multichannelmerchant.com/marketing/instagram-breeding-ground-counterfeit-products/specific and the product of the pr

https://www.trademarks and brands on line.com/article/brand-protection-on line-what-you-need-to-known and the compact of the protection of the compact of

https://blog.redpoints.com/en/the-ultimate-guide-to-brand-protection

https://www.forbes.com/sites/roomykhan/2019/05/10/counterfeits-amazon-etsy-ebay-instagram-and-others-duping-consumers-and-damaging-innovation/#57b7a2106002 https://www.geekwire.com/2019/amazon-sues-alleged-international-counterfeiting-ring-escalating-battle-knock-off-products/



Digimarc Corporation

9405 SW Gemini Drive
Beaverton, OR 97008
T: +1 800 DIGIMARC (344,463

F· +1 503 469 4777

info@digimarc.com www.digimarc.com

© 2019 Digimarc Corporation

ABOUT DIGIMARC CORPORATION

Digimarc Corporation (NASDAQ: DMRC) is a pioneer in the automatic identification of everyday objects such as product packaging and virtually any media, including print, images and audio. The Digimarc Platform provides innovative and comprehensive automatic recognition technologies to simplify search, and transform information discovery through unparalleled reliability, efficiency and security. Digimarc has a global patent portfolio, which includes over 1,100 granted and pending patents. These innovations include state-of-the-art identification technology, Digimarc Barcode, as well as Digimarc Discover® software for barcode scanning, image recognition, as layers of its ground-breaking Platform. Digimarc is based in Beaverton, Oregon. The Digimarc Platform enables applications that benefit retailers and consumer brands, national and state government agencies, media and entertainment industries, and others. Visit digimarc.

