Enforcing Your IP on Independent Websites

Every unauthorised website or imitation web store siphons potential revenue and erodes consumer trust. In a digital landscape where fraudulent domains can be launched in minutes, protecting your brand's online presence isn't optional; it's a commercial necessity to ensure your customers remain safe.

Independent websites—those operating outside of major marketplaces like Amazon or eBay—present a unique challenge for brand protection. Because there is no central marketplace authority to appeal to, enforcement requires a more technical approach. To maintain your brand's integrity, you must move beyond simple monitoring and target the infrastructure that keeps these fraudulent sites online.

Step 1: Assess and Verify the Threat

Speed is vital. Use software to scan for domain names that mimic your brand or use your registered trademarks. Verify the threat by identifying "Super Threats"—high-traffic sites that use your official imagery, logos, and product descriptions to deceive customers.

Step 2: Gather Digital Evidence

Before the site can change or disappear, capture a "chain of evidence." Take time-stamped screenshots of the homepage, checkout, and contact pages. Document the nature of the abuse, such as phishing, counterfeit sales, or trademark squatting.

Step 3: Identify the Infrastructure

Since there is no "Report" button, you must find where the site lives. Use WHOIS lookups and technical tools to identify the Hosting Provider (the digital landlord) and the Domain Registrar (the company that registered the URL).

Step 4: Target the Hosting Provider

The hosting provider has the power to "pull the plug." Submit a formal report to their abuse department or a DMCA takedown notice. Detail the specific unauthorised use of your IP and provide the direct URLs of the infringing content.

Step 5: Contact the Domain Registrar

You will be asked to provide an electronic signature before submitting. Once submitted, you will receive a confirmation email with a unique reference number. Keep this for your records to track the status of the report

Step 6: Cut Off Payments and Traffic

If the site persists, escalate by reporting the fraudulent activity to payment processors and search engines. This makes it harder for the site to process transactions or appear in customer search results.

Step 7: Review and Prevent

Move from reactive to proactive. Regularly audit new domain registrations and provide staff training on spotting "look-alike" domains. Work with registrars to prevent the "shock and violation" of recurring brand abuse.

What Happens Next?

Infrastructure providers require "clean," documented evidence to act. If your report is successful, the site will be disabled or the domain suspended. Properly documenting and protecting your rights is the best way to prevent future unauthorised use and safeguard your brand’s global digital footprint.

Contact Us

SnapDragon combines AI-powered detection, expert enforcement, and global experience to keep counterfeits off the market and your genuine products where they belong – in customers' hands.

Talk to SnapDragon about how proactive brand protection can drive stronger, more sustainable growth.

www.snapdragon-ip.com

UK & RoW: +44 131 466 9249
US: +1 857 400 7041

thelair@snapdragon-ip.com

LinkedIn

SnapDragon