Special Edition 2011

Brandjacking Index®

Sports Apparel Online

MarkMonitor®
PART OF THOMSON REUTERS

Brandjacking Index®

Special Edition 2011 - Sports Apparel Online

Contents

Executive Summary

If you are looking to buy sports apparel such as a shirt or jersey with the logo of your favorite league, chances are good that you will encounter a counterfeit. Online fraudsters see a tremendous opportunity in the passion and loyalty of millions of sports fans who may be located all over the world but who are united by a single bond: love for their team. These fraudsters make easy money by selling popular—and unlicensed—apparel to these loyal fans.

We found more than 6,000 suspects selling more than 1.2 million shirts or jerseys annually over the Internet, generating nearly $25 million in revenue. The e-commerce sites selling this suspicious apparel attract 56 million annual visits.

"Online fraudsters see a tremendous opportunity in the passion and loyalty of millions of sports fans."

Along with their distribution prowess, these fraudsters display a high level of sophistication to attract traffic to their sites. They invest heavily in paid search advertising, occupying almost 28% of all ads triggered by branded keywords and funneling an estimated 11 million annual visits to their sites from this marketing method alone. They are adept in search engine optimization (SEO), using 'black hat' techniques to boost organic search results for these suspicious sites.

We also discovered almost 500 cybersquatted sites using other monetization techniques, including pay-per-click ads and questionable affiliate marketing practices, to capitalize on major sports brands for their own financial gain. All this makes it harder for fans to find the real apparel sold by legitimate vendors that are authorized by the sports brands when shopping for this kind of clothing online.

In this edition of the Brandjacking Index®, we analyzed five major sports brands, including US leagues and international competitions, to see who was using these brands in online trading and promotion of sports apparel with questionable provenance. We didn't look at individual team brands or other sports-related offerings such as shorts and caps, tickets or live game video streams: our objective was to measure just a very specific market segment and determine what kind of abuse exists for these leading brands.

As is the case with our previous Brandjacking reports, we examined a variety of online channels including business-to-business (B2B) sellers of bulk goods and business-to-consumer (B2C) sites, including e-commerce sites, along with more than 300 branded keyword combinations that triggered paid search ads across major search engines. We conducted this research during the last quarter of 2010, examining the traffic generated by the suspicious sites and the methods used to ensnare consumers.

Key Findings

It isn't hard to find fraudsters targeting the online sports apparel business. The sheer size of the abuse puts this market into a major league of its own.

For the five brands in the study, we identified more than 1,300 e-commerce websites, the vast majority of which were linked to a Chinese registrant or registrar, selling questionable sports apparel. Those e-commerce sites alone attracted more than 56 million annual visits. Using industry metrics for order conversion, we estimate that these sites are selling 800,000 units of suspicious sports apparel annually.

> *"Sites selling this suspicious apparel attract 56 million annual visits."*

We also discovered twelve B2B exchange sites with more than 4,000 individual, unauthorized suppliers that appear to be offering phony merchandise. This supply chain consists of suppliers who are based predominantly in Asia and are estimated to sell 300,000 shirts or jerseys annually.

B2B Market Listing

Aside from the sheer volume of merchandise, the level of online marketing savvy displayed by these questionable sports apparel sellers is high. They are adept at using best practices in online marketing techniques to take advantage of the dedicated fan and the naïve consumer. These questionable merchants use the basic methods that any customer can use to locate an online merchant but exploit those methods for their own ends:

- **Direct navigation**, by typing in the domain name in their browser. By purchasing cybersquatted domains that are nearly the same as the established brand and to which they have no rights, such as sportsbrandx4cheap.com, they can masquerade as the actual sports brand, when in reality, they have no such relationship.

- **Organic search**, by promoting their sites using 'black hat' or questionable means, these deceitful sites can rise to the top of the search results pages and gather clicks and traffic. These 'black hat' techniques include unauthorized use of the actual brand in their domain names, page titles and other meta tags as well as cultivating a large number of inbound links from 'splog' or spam blog sites to trick the search engines into thinking that they are popular sites.
- **Paid search advertising**. The phony vendors buy branded keywords to trigger paid search ads, just like the actual sports brands do.

"More than 130,000 ads promoted suspicious goods, driving an estimated 11 million annual visits."

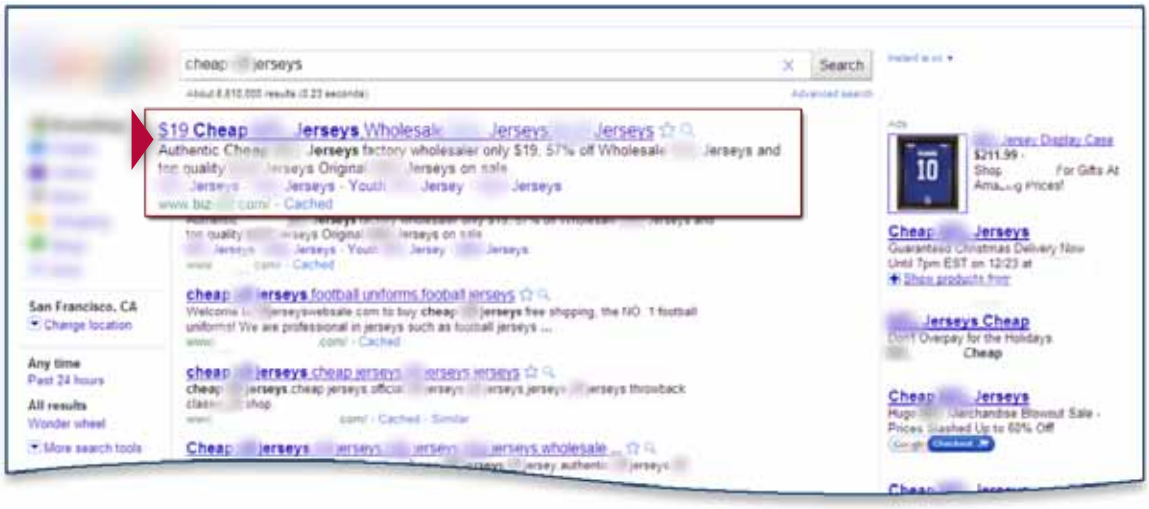
For example, let's look at doing a search on "league x jerseys online" in a popular search engine. The first page of results brings up 11 ads, of which three are suspicious, including the top paid ad position. During the study period, we examined almost 480,000 paid search ads, triggered by more than 280 keyword combinations. We found almost 28% of these ads, or more than 130,000 ads, promoted suspicious goods. These ads drove an estimated 11 million annual visits.

Paid search ads lead to sites selling fakes and enjoy top positions

This means that suspected counterfeiters are competing with legitimate advertisers for advertising inventory, driving up prices and even outbidding legitimate advertisers for premium placement. As a result, the legitimate advertisers have to pay more for their search keywords and compete with counterfeiters for traffic seeking their brands.

This is especially noteworthy when considering that 20% of all searches are for trademarked terms, according to a recent comScore and Yahoo Search Marketing (Overture) study.

Another traffic generation technique used by these fraudsters is to promote their sites in organic or non-paid search results, using inbound links from questionable sites like spam blogs, or 'splogs', to further exploit search engine results. These splogs copy legitimate content from elsewhere on the Web and contain a high number of links to exploit search algorithms. Here is one example of this technique where all of the organic search results on this page are links to sites selling suspected counterfeit shirts or jerseys. One of the results has nearly four thousand inbound links from other sites, some of which are cybersquatted splogs.

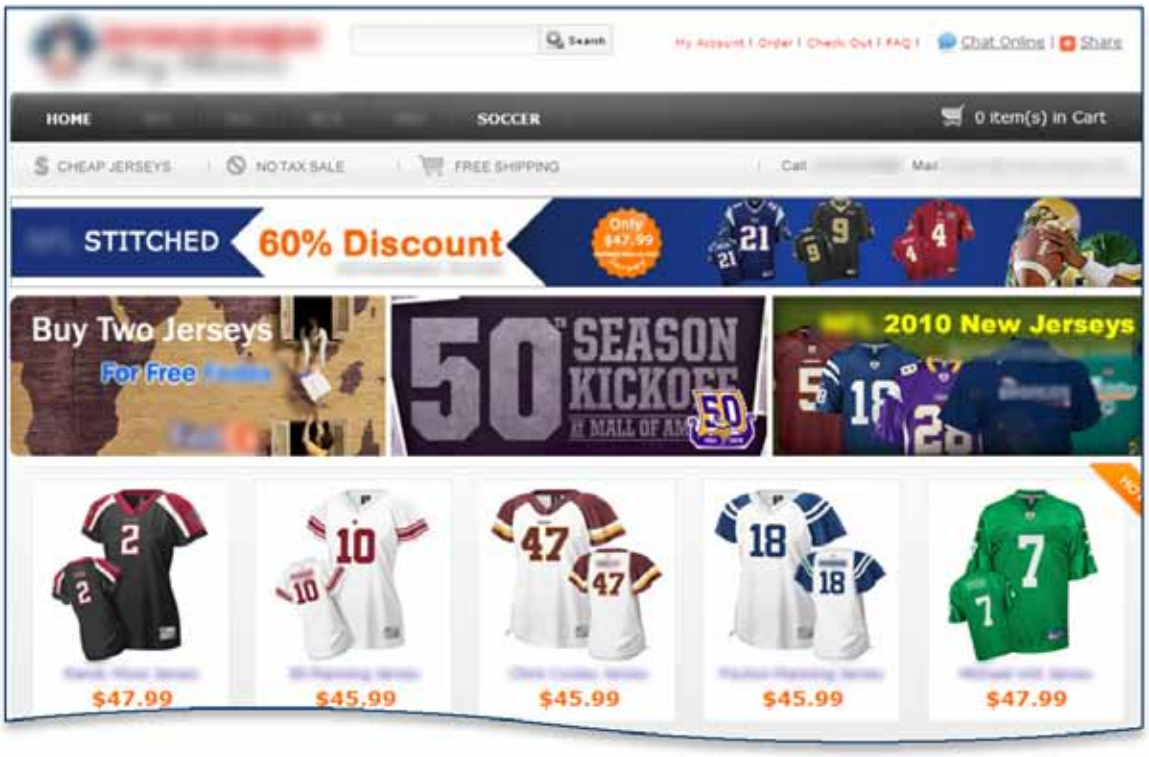


Black hat SEO techniques used to boost organic rankings

Certainly, there are legitimate sites that offer sports apparel at discounted prices, but the results found in our study highlight questionable practices, indicating levels of counterfeiting and other suspicious activity that is on par with the most sophisticated fraudsters we've analyzed in other industries.

For example, this site offers deep discounts on many different team and league logoed apparel. Its domain name is registered by a Chinese registrar and the site receives almost three million visits annually, based on Alexa data. None of the items sold on this site are officially licensed by the sports brands.

> *"Suspected counterfeiters are competing with legitimate advertisers for advertising inventory"*



E-commerce site sells counterfeit sports apparel from multiple brands, attracts significant traffic

There are many cases of mixing fraudulent and legitimate sellers in a complex web that makes it hard even for the discerning consumer to understand fair from foul play. For example, a cybersquatted site redirects a visitor to an authorized dealer's site. That authorized dealer, then, is leveraging the traffic of the cybersquatted domain to drive their own revenue. The amount of traffic that can be generated off the back of a cybersquatted domain can be significant—sometimes up to several million annual visits.

Another technique that can confuse those seeking sports-branded apparel is in the realm of affiliate marketing. For example, an affiliate marketer registers a cybersquatted domain involving a major sports league brand and then links to popular retail and auction sites, redirecting traffic to unauthorized channels. In return, the affiliate marketer is compensated for all traffic that converts to a sale on these unauthorized B2C sites and the consumer potentially (and unknowingly) ends up buying non-authentic merchandise.

Summary

The amount of business generated by e-commerce sites selling suspicious sports apparel is significant. The operators of these sites are online marketing savvy, drive millions of visits to their sites and generate significant revenue. Thousands of sellers earn millions of dollars in annual sales of apparel that isn't licensed by the sports brands. Sadly, because of the sheer number of questionable sites and the sophisticated effort put into promoting them by their operators, sports brands must compete with counterfeiters for sales of their own brands. It is essential that brands craft enforcement strategies that attack not only the online distribution of their goods but also their online promotion in order to address this multi-million dollar problem and to help their loyal fans to display their team spirit with authentic goods.

Methodology and Background

The Brandjacking Index is produced by MarkMonitor® and analyzes trends and statistics about brand abuse online as well as anecdotal information about the business and technical methods used by brandjackers. The cornerstone of the Brandjacking Index is the volume of public data analyzed by MarkMonitor using the company's proprietary algorithms. None of this data contains proprietary customer information.

This special edition of the Brandjacking Index drew conclusions based on data from major search engines, online marketplaces, Whois records and Alexa traffic estimates.

Glossary

Brandjacking – To hijack a brand to deceive or divert attention; often used in abusive or fraudulent activities devised for gain at the expense of the goodwill, brand equity and customer trust of actual brand owners.

Black Hat SEO – The use of brands, slogans or trademarks located in visible text, hidden text, meta tags and title in order to manipulate search engine rankings so that the brandjacker's site can gain a more favorable search engine placement.

Cybersquatting – The practice of abusing trademarks within the domain name system.

Domain Kiting – The process whereby domains are registered and dropped within the five-day ICANN grace period, and then registered again for another five days. Kiting a domain lets the registrant gain the benefit of ownership without ever paying for the domain.

eCommerce Content – Websites containing a specified brand that appears in visible text, hidden text, meta tags or title in conjunction with other site content that indicates online sales are being transacted on the site.

False Association – The practice of using a specified brand or trademark in web content to imply a relationship with a company or brand where none exists.

Offensive Content – Websites containing a specified brand that appears in visible text, hidden text, meta tags or title in conjunction with pornographic, online gaming or hate content.

Paid Search Scams – Occur when a brand is used without permission, within a paid search scenario to drive web traffic to a competitive or illicit site.

Phishing – Criminal use of email to divert traffic to websites in order to fraudulently acquire usernames, passwords, credit card details and other personal information. The email and websites used in these operations employ "social engineering" techniques to trick users into believing they are interacting with a business or organization that they trust.

Rock Phishing – A method of phishing first implemented by the 'rock' phish gang that utilizes multiple layers of redundant infrastructure to increase the difficulty of shutting down the attack. Other phishers are now using these tactics as well.

About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its patented real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today. For more information, please visit **www.markmonitor.com**.

More than half the Fortune 100 trust MarkMonitor to protect their brands online.
See what we can do for you.

MarkMonitor Inc.
U.S. (800) 745-9229
Europe: +44 (0) 207 840 1300
www.markmonitor.com

San Francisco | Boise | Washington, DC | London

MarkMonitor®
PART OF THOMSON REUTERS