

BrandSecure® News

Inspired by Technology. Proven by Experience® | Winter 2011



This issue of BrandSecure News presents Enterprise Brand Protection as a strategic business initiative. We give an abstract of OpSec's market analysis of the online marketplace for pharmaceuticals. We also feature Xerox's integrated brand protection program, and highlight ICE's Cyber Monday crackdown on rogue online retailers.

The Strategic Value of Enterprise Brand Protection™

During this season of consumer spending, every business is in high gear working to meet customer demand and maximize revenue potential. However, the opportunity to make a profit also attracts illegitimate entities peddling counterfeit and grey market goods.

Status Quo of Brand Protection

Silos of brand protection activity abound as each function in an organization is on alert to fortify security measures within its jurisdiction. Corporate security works with local law enforcement to raid "bargain" stores and flea markets, and coordinates with customs officials to seize counterfeit cargo. The legal team shuts down infringing auction listings, and sends out warning letters for unauthorized use of trademarks. Sales and marketing monitor pricing variations across regions, and identify channel partners out of compliance.

Companies have varying levels of coordination amongst functional teams, and some benefit from a brand protection group. More often than not, brand protection is short on staff, low in budget, and tactical in focus. While the potential risks are great, brand protection is seen as an expense that is difficult to justify.

Paradigm Shift to Enterprise Engagement

For a commercial enterprise, an investment in brand protection should come from a strategic analysis of the financial risks and bottom-line impact of counter-

feiting and grey market diversion. The value of brand protection is best created by a holistic engagement of business functions across the enterprise.

Enterprise Brand Protection is a strategic enterprise-wide engagement



Enterprise Brand Protection is driven by revenue optimization of strategic business objectives. It is a coordinated response to corporate risks in consumer health and safety, breaches in supply chain security, breakdowns in product integrity, damage to brand image, and revenue loss.

Business Analysis for Enterprise Optimization

The starting point for Enterprise Brand Protection is a strategic evaluation of risks from infiltration by counterfeits, grey market diversion, online channels, and intellectual property (IP) infringements.

- Audit Supply Chain and Product Security Processes to analyze gaps in manufacturing, packaging, and distribution, identify

In This Issue

- OpSec Study Reveals Increased Risks of Counterfeit Pharmaceuticals in the Online Marketplace
- Xerox Fights Grey Market Diversion with an Integrated Brand Protection Strategy
- ICE Seizes Websites Selling Counterfeits on Cyber Monday Crackdown

product packaging and labeling solution components, and examine needs for product tracking data

- Conduct Internet Landscape Analysis to gather intelligence on product availability, and assess level of risk exposure
- Assess IP Enforcement Procedures to review worldwide IP portfolio, evaluate investigative strategies and field testing programs, and find opportunities for more effective IP enforcement

Enterprise Brand Protection is a coordinated drive for revenue optimization



Enterprise Brand Protection examines processes and solutions for an integrated program of product authentication, product tracking, online monitoring, and IP enforcement. The result is an identification of deficiencies and a prioritization of opportunities to optimize revenue potential and achieve measurable ROI.



OpSec Study Reveals Increased Risks of Counterfeit Pharmaceuticals in the Online Marketplace

OpSec conducted a market study to identify the latest trends and key developments in the online marketplace for pharmaceuticals. The findings show that the illicit practices of Internet pharmacies and Business-to-Business (B2B) trade board sellers expose



consumers and the global supply chain to greater risks from counterfeit drugs, bulk pharmaceuticals, and active pharmaceutical ingredients (APIs).

The current analysis is part of OpSec's ongoing monitoring of the pharmaceutical landscape, and adds to the insights gained from the earlier two-year study conducted from 2007 to 2009.

Rogue Internet Pharmacies Use Deceptive Practices to Target Consumers

- **Use of message board spamming to selectively target consumers searching for controlled substances online.** In this technique, a rogue pharmacy simultaneously sends a link offering highly regulated drugs, such as Oxycontin and Adderall, to hundreds of popular message boards. This method increases the visibility of the spammed links in search engine results, and diverts consumers to illegitimate offers of substandard or counterfeit scheduled drugs.
- **Covert marketing of controlled substances by rogue marketing affiliates on offshoot storefronts.** Many rogue marketing networks sell only non-scheduled drugs on their highly visible websites, but operate seemingly unrelated sites selling other products as a cover to market controlled substances. In one example, the Customer Care webpage of a website purported to be selling consumer electronics offers highly regulated drugs, such as phentermine and zolpidem.

- **False affiliation to give rogue websites appearance of legitimacy.** Rogue pharmacies are exploiting U.S. consumer trust in Canadian online pharmacies as safe alternatives for affordable medicine. 94% of Internet pharmacies purport to be Canadian. Some visibly place the Canadian maple leaf icon on the site page header. Others falsely claim to be accredited by the Canadian International Pharmacy Association, which certifies all qualified Canadian Internet pharmacies. However, 20% of sites claiming to be Canadian are not registered in Canada, but in counterfeit hotspots like Russia, Panama, and Bulgaria.
- **Offers of discounted prices for generic versions of prescription drugs still under patent.** 72% of rogue Internet pharmacies offer generic versions of drugs still under U.S. patent protection for shipment to U.S. patients. Often, these generic medicines are manufactured in India, a country known for cut-rate prices and potentially substandard quality.

Internet Pharmacies and Trade Board Sellers Exhibit Increased Trends of Illicit Behavior

The study identified growing trends of rogue behavior by Internet pharmacies selling drugs to consumers, and trade board sellers offering bulk pharmaceuticals and APIs into the global supply chain.

- 86% of unaccredited online pharmacies offer drugs with discounts of 40% or more, up from 42% in 2007
- 89% of unaccredited online pharmacies do not require a prescription, up from 51% in 2007
- 79% of unaccredited online pharmacies have U.S. site registrations, up from 55% in 2009, although this positive trend is offset by the corresponding practice of using blatantly false information, such as celebrity names as registrants
- Increasing number of B2B trade board sellers are positioning themselves as drop shippers or order fulfillment centers for Internet pharmacies
- 90% annual increase in trade board listings of bulk pharmaceuticals for sale on B2B platforms
- Significantly expanded drug and API portfolios from manufacturers and distributors from China and India selling on B2B trade boards
- 50% annual increase in listings from trade board sellers outside of China and India, mostly from Eastern Europe, Malaysia, and Turkey

The findings of the OpSec study reveal escalated risks to patient safety and the pharmaceutical supply chain. Whether the appeal is from easy access, discounted prices, or the appearance of legitimacy, consumers who are purchasing drugs online need to be wary. The increasing penetration of counterfeit pharmaceuticals into the online marketplace is a growing concern that requires the attention and coordinated response of government agencies, pharmaceutical industry, and consumer advocacy groups.



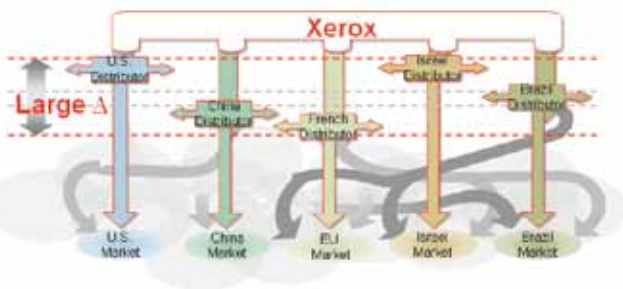
Xerox Fights Grey Market Diversion with an Integrated Brand Protection Strategy

Business Challenges

Xerox is the world's leading enterprise for business process and document management. With 133,000 employees and annual revenues of \$22 billion, Xerox offers office products, production equipment and business services to companies worldwide. Xerox' Brand Protection Group in the Supplies business is charged with the mission to protect Xerox' intellectual property and minimize consumables revenue loss to grey, black and aftermarket activities.

Grey market diversion was a growing concern that was driven by Xerox' two-tier go-to-market strategy. A price arbitrage exists when wholesale prices vary from price harmonization guidelines. The grey market represents the unauthorized sale of Xerox products or the diversion of Xerox products from authorized distribution channels. As a result, channel relationships, sales revenues and customer perception were negatively impacted. Xerox developed measurements which suggested that grey market diversion costs millions of dollars in revenues.

Inconsistent pricing strategies create incentives for grey market diversion



OpSec Solution

With the support of senior management, Xerox formulated key strategies to combat the grey market which included price harmonization, development and support of regionalized products, and shipment controls. Xerox selected OpSec Security to support its initiatives in combating grey

and black market challenges. OpSec's integrated BrandSecure® solutions enabled Xerox to implement proactive measures and monitoring capabilities across the supply chain.

OpSec's integrated BrandSecure® solutions supported Xerox' brand protection strategy.



Product Authentication



Product Tracking



Internet Monitoring

Xerox implemented OpSec's anti-counterfeiting, product tracking, and Internet monitoring solutions for its Supplies business. As the first line of defense against counterfeiting, a high-security authentication label was deployed for Xerox consumable products worldwide. The authentication label is designed with features to enable product tracking across distribution channels, partners, and resellers. Product serialization is applied at the item level to track product and shipment information at each node of the distribution network. Using the

tracking system, Xerox is able to identify the occurrence of theft, reseller diversion, or internal operating company diversion. In addition, OpSec's Internet monitoring services provide business intelligence for pricing studies against harmonized guidelines, analysis of product availability on trade boards, and identification of sales diversion from trademark infringements.

Business Benefits

Xerox notes progress in the fight against grey market diversion. The availability of unauthorized resellers is reduced; prices in unauthorized channels are normalizing; and trends on gross margin and revenues are improving.

In one case study, Xerox began a program to mark goods prior to shipment to a suspect partner. These same marked goods were found in non-authorized geographies and confirmed suspicions of grey market diversion. Subsequent analysis of partner volume needs revealed overshipment of products by more than 30%. Xerox shared these fact-based findings with the partner and implemented shipment controls to stop the leakage.

Xerox remains committed in its fight against grey and black market activities. Tools and processes are in place to establish tighter supply chain control and capture the maximum benefits of its brand protection efforts. Since implementing its grey market diversion strategy, Xerox' Brand Protection Group has made significant impact on the company's bottom line.

"There is a strong need for consolidation in the brand protection marketplace. To date, this industry has been fragmented, requiring companies like ours to seek multiple vendors to satisfy our product protection requirements. OpSec's multinational presence and ability to deploy product marking solutions, combined with its professional services and software solutions bring value to companies looking for a comprehensive, integrated solution to address their brand protection needs."

– Xerox Corporation



ICE Seizes Websites Selling Counterfeits on Cyber Monday Crackdown

On Cyber Monday following Thanksgiving weekend, U.S. Immigration and Customs Enforcement (ICE) executed seizure orders against 82 commercial websites engaged in the sale and distribution of counterfeit products and copyrighted works. Operation in Our Sites v. 2.0 was timed to disrupt counterfeit sales on the busiest online shopping day of the year.

The domain name seizures targeted online retailers selling a range of counterfeit goods, including apparel, handbags, shoes, sporting goods, and sunglasses as well as pirated DVDs, music, and software. During the course of the investigation, officials conducted test purchases from suspect sellers. Many of the counterfeit goods were shipped into the U.S. from other countries. If the goods were found to be counterfeit or illegal, seizure orders were obtained.

Attorney General Eric Holder announced the seizures as part of a larger federal initiative to protect the interests of consumers and trade. ICE Director John Morton indicated ICE's priority to protect intellectual property, and take action against rogue online commerce. All 82 sites were shut down and display a web banner noti-

fying visitors that federal authorities had taken control of the domain name.



Web banner on sites of seized domain names

This enforcement action follows Operation in Our Sites I, announced in June 2010, which targeted websites offering pirated movies and streaming videos. Both operations were the result of federal law enforcement coordinated by the National Intellectual Property Rights Coordination Center, led by ICE's Office of Homeland Security Investigations, and in cooperation with the Department of Justice. The nationwide operations send a message to illicit seller networks that counterfeit commerce will not be tolerated, and warns consumers to beware of deceptive online practices.

Source: www.ice.gov

Events

2011 International CES

January 6-9, 2011 Las Vegas, NV

www.cesweb.org

Bread & Butter (Winter)

January 19-21, 2011 Berlin, Germany

www.breadandbutter.com

Outdoor Retailer Winter Market

January 20-23, 2011 Salt Lake City, UT

www.outdoorretailer.com/winter-market

IQPC Anti-Counterfeiting & Brand Protection West Coast

January 24-26, 2011 San Francisco, CA

www.anticounterfeitingsummit.com

Global Congress: Combating Counterfeiting & Piracy

February 2-3, 2011 Paris, France

www.ccapcongress.net

ISPO

February 6-9, 2011 Munich, Germany

www.ispo.com

CeBIT

March 1-5, 2011 Hannover, Germany

www.cebit.de

MIPEL

March 6-9, 2011 Milan, Italy

www.mipel.com

BaselWorld

March 24-31, 2011 Basel, Switzerland

www.baselworld.com

Interpharm

March 25-27, 2011 Hamburg, Germany

www.interpharm.de

Published By

OpSec Security, Inc.

3 Copley Place

Suite 201

Boston, MA 02116

P 617.226.3000

F 617.226.3001

www.opsecsecurity.com

Editor

Terri Mock

Vice President, Global Marketing

Email: tmock@opsecsecurity.com

