

BrandSecure™ News

Inspired by Technology. Proven by Experience® | Winter 2010



The Winter issue of BrandSecure News focuses on the consumer electronics and technology sectors. We discuss the challenges manufacturers face in their battle against the unauthorized distribution of genuine products and the illegal infiltration of counterfeit goods into their distribution channels.

Keep Out Grey Market and Counterfeit Goods

Infiltration of the Distribution Network

From the latest cool gadgets to popular models of electronic devices, manufacturers are in constant vigilance to combat grey market diversion of their products. It involves the sale of new, branded goods in unauthorized distribution channels or the importation of these goods into other regions without the manufacturer's permission.

"Grey market sales of IT products account for over \$40 billion in annual revenues, and result in an estimated \$5 billion of lost profits to manufacturers each year."

Study by KPMG and the Alliance for Gray Market and Counterfeit Abatement, February 2003

Additionally, manufacturers are also on guard against counterfeit products entering the legitimate supply chain. Such counterfeits consist of finished products, component parts, or packaging, and constitute illegal infringements of the manufacturer's trademark. When counterfeits are introduced into the grey market infrastructure, they further add to the risk of channels and consumers receiving fake, substandard, and altered goods. For example:

"A recent quality audit of 31 manufacturers of cell phone components by the Guangdong Administration for Industry and Commerce reported that only 65%

of the mobile phone batteries sold in the market were up to standard."

SOSCO IPR Insight No. 2, Nov 2009

The infiltration of grey market and counterfeit goods raise significant challenges. Such illegal and nefarious activity can quickly compromise product integrity, undermine legitimate sales channels, sabotage customer satisfaction, undercut sales revenues, increase warranty costs, and tarnish brand image.

Protecting Authorized Channels

Manufacturers can apply the ABCs of brand protection to protect authorized channels and limit their exposure to grey market and counterfeit goods.

Assess the Problem – Develop measurements to better understand the extent of the grey market diversion

- Financial Metrics, e.g. analyze orders and revenues by geography compared to forecasts
- Marketplace Intelligence, e.g. monitor pricing and availability of products in online channels
- External Audits, e.g. survey goods from various channels and geographies

BrandSecure® Your Products – Implement an integrated brand protection strategy to combat counterfeiting and diversion using OpSec's BrandSecure solutions

In This Issue

- OpSec Study Integrates Social Media and E-Commerce Monitoring to Combat Unauthorized Online Sales
- Lenovo Leverages Internet Monitoring to Expose Grey Market Sales and Wholesaler Fraud
- Microsoft and OpSec Security Uncover Pirate Copies on Auction Portals
- Authenticate – Defend against counterfeiting by authenticating genuine goods
- Track – Trace products on the item-level for diversion into the grey market
- Monitor – Analyze online channels and e-commerce platforms for suspect products, sellers, and distribution networks

Control the Leaks – Act to deter leakage out and infiltration into the legitimate supply chain

- Implement shipment controls to stop leakage
- Administer inventory controls of components and finished goods
- Enforce contract compliance with non-compliant distributors
- Pursue legal action against IP infringers with law enforcement
- Educate the sales team and authorized distribution channels

Manufacturers can take steps to significantly reduce unauthorized sales in the grey and black markets.



OpSec Study Integrates Social Media and E-Commerce Monitoring to Combat Unauthorized Online Sales

OpSec Security conducted a study to identify the impact of Internet trading platforms and social media web forums on the market launch and distribution of consumer electronics products. As new products are introduced into the global marketplace, monitoring popular B2C auctions, B2B trade boards, blogs and forums provides significant intelligence about the emergence of grey and counterfeit markets.

The study focused on Kindle e-readers and the market launch of Amazon's DX model introduced on June 10, 2009.

- On launch day, Kindle DXs were already available for purchase on a major B2B trade board from a company located in China
- A sample of 8 seller listings on a popular trade board had an estimated 40,000 Kindles available within a few weeks after the DX launch
- Suspect Kindle knockoffs were found for sale on trade boards and auctions in colors and languages not sold by Amazon
- Consumers used social media forums to share tips on circumventing Amazon's U.S. only shipping restrictions, including the use of package forwarding companies

Assess Trade Boards and Auctions for Counterfeit and Grey Market Activity

The product launch of a highly anticipated consumer electronics product, such as the Kindle DX, presents a major challenge to manufacturers desiring to maintain supply chain control in the global market. Even on the day of launch, Kindle DXs were offered for sale on a B2B trade board raising questions on how the product was acquired (Figure 1).

Of the thousands of Kindle e-readers that surfaced on trade boards, many were selling substantially below the retail price. One seller offered 2,500 Kindle 2 e-readers per week at a unit price of \$65, well below the list price of \$299 (Figure 2). Of 33 B2B listings offering Kindles when the DX

launched, 75% of the sellers were located in Indonesia and China.

A grey market quickly grew of auction sellers offering the Kindle DX at premium prices to meet the demands of consumers in regions who could not buy from Amazon. In the four months since the launch, the quantity of Kindles (all models) available on eBay increased almost three-fold from 1,776 units to 5,092 units, including a ten-fold increase for the DX version from 268 units to 2,970 units. In addition, black and Japanese language Kindle knockoffs were found, neither of which are offered by Amazon. These findings give impetus to monitor e-commerce platforms to identify black and grey market goods entering the supply chain.

Monitor Social Media for Product Availability and Consumer Sentiment

The study monitored social media platforms for comments on how to circumvent Amazon's shipping restrictions for the Kindle. Until the recent announcement of the international Kindle 2 and DX versions, Amazon did not ship Kindles outside the U.S.

ing through family and friends, a popular strategy was to find an e-Bay seller that shipped internationally. Another popular approach was the use of a forwarding company. This service circumvented Amazon's restrictions by shipping the product to a U.S. address, and then forwarding it to the buyer's international address. In addition, the large majority of DX listings were posted at premium prices indicating the willingness of buyers to pay extra. The findings from social media and e-commerce monitoring provided online intelligence on the demand from international buyers and the growth of the grey market.

Use Internet Intelligence to Understand Global Product Distribution

The growth of the Internet as a global marketplace and a worldwide user community means that future product launches of consumer electronics will be accompanied by the rapid emergence of grey and counterfeit markets. This will only become more prevalent as the Internet is used to purchase and promote products, thereby establishing a market for distributing unauthorized and counterfeit goods. Combining market intelligence



Figure 1



Figure 2

Consumers shared information about online sellers, recommended vendors, and ways of obtaining Kindles in countries where they were not intended to be sold. Other than the obvious method of order-

from e-commerce platforms and social media enables companies to quickly and effectively respond to the emerging threats of counterfeit and grey market goods.



Lenovo Leverages Internet Monitoring to Expose Grey Market Sales and Wholesaler Fraud

The Internet is gaining importance as a distribution channel. What challenges lie ahead for Lenovo in the sale of its products on the Internet?

D. Klein: Our largest task is combating grey market sales. In addition, we are facing stiff competition from aggressively priced offers on our goods on the Internet. One example of what we are facing is very aggressive offers of Lenovo peripherals on price search engines such as idealo.de and geizhals.at. In reviewing these websites, we discovered a large number of docking stations at suspiciously low prices. Their availability were not well-received by our business customers who had purchased similar units from us at higher prices. Also, our channel partners were concerned about losing revenues to unauthorized online shops.

What measures have you taken to identify suspicious offers and dealers on the Internet?

D. Klein: In cooperation with OpSec, we search the Internet – in particular, well known price search engines – for dubious offers. From our Internet monitoring activities, we have found examples of grey market imports, non-compliance in our delivery timetables, loss leader prices, violations of the Waste Equipment Act, and wholesaler fraud.

The real detective work begins once we encounter a suspicious offer or suspect online shop: Do we know the shop? Are we already working with them? What is the price structure of the online offer? How do other online vendors sell the product? In the example cited earlier, we worked with OpSec to conduct a series of test purchases that allowed us to trace the source of the docking stations. It turned out that one distribution partner had breached the terms of its contract, and was selling discounted wholesale bundles to consumers (the end customers) in quantities greater than those agreed. A subsequent audit then allowed us to

expose the extent of the unauthorized sales and calculate the level of contractual penalty due.

As this example shows, test purchases are extremely important for us. We are able to establish the origin of goods through their machine and serial numbers. This provides us with crucial evidence in identifying possible cases of fraud. We also came across foreign products in the course of our research and were able to assist our European colleagues in combating grey market sales.

How do you proceed against dubious online vendors?

D. Klein: First, we speak to the online distributors directly and attempt to resolve the case with them. For instance, our contractual partners are obliged to contact Lenovo if an end consumer does not purchase all devices in a discounted bundle package offer. In such a case, we are happy to find a solution and come to an agreement with our business partner. If, however, a particular online distributor violates the terms of their contract, strict penalties and consequences ensue.

Theoretically, each individual product from a discounted package has to be sold to an end consumer and documented as such. For each product that the online vendor is unable to provide documentation of an authorized sale, the trader is required to pay a contract penalty of 30 percent of the manufacturer's suggested retail price. When an intentional breach of contract has transpired, this can lead to the termination of the business partnership.

How effective has your approach been in combating grey market sales and wholesaler fraud?

D. Klein: Our work with OpSec enables us to control our online sales. We are also able to optimize our online channels, and ensure that our price structure is not



Biography:

Dorothee Klein has been working for Lenovo for over three years. After two years managing the profitability of major projects, she currently directs the relationships with distribution partners and leads efforts to combat the impact of grey market diversion.

undermined. In addition, we increasingly receive positive feedback from authorized vendors who value our commitment to the removal of unauthorized or non-compliant distributors. As our work in this area has been extremely successful, we now plan to utilize it to a greater extent throughout Europe.

Interview with Dorothee C. Klein, Transactional Business Operations Germany/Austria, Lenovo GmbH

Microsoft and OpSec Security Uncover Pirate Copies on Auction Portals

OpSec Security and Microsoft Deutschland GmbH are working together to combat the increasingly illegal sale of counterfeit software via auction websites. An IDC study commissioned by the Business Software Alliance (BSA) has shown that the piracy rate in Germany is currently around 27 percent, which amounts to software valued at €1.55 billion. These pirate copies also represent a threat to consumers as they often contain viruses, spyware or Trojans. Software piracy greatly affects the development of the IT industry, one of the most important sectors for the German economy.



When searching online trading portals and internet auction sites such as eBay or hood.de for counterfeit or unlicensed software postings, OpSec uses its proprietary automated search technology to identify suspect pirate copies. The suspicious products filtered by the software are then manually examined by OpSec Security. "If our suspicion that the product could be a pirate copy is further substantiated, we then implement national and international test purchases," explains Hubert Neuner, Managing Director of OpSec Security. "The anonymous test purchases

provide us with important information on the seller. In addition, Microsoft can clarify beyond a doubt that the purchased products are original software or indeed pirate copies and then take further action against the specific seller of the illegal software."

In close cooperation with OpSec Security, Microsoft's Product Identification Service (PID) then carefully examines the offers which have been filtered out, for genuineness. "Through our work with the trade mark protection experts of OpSec Security, we have already been able to register considerable success in our battle against online piracy," said Joachim Rosenoegger, Microsoft Germany's Anti-Piracy Investigator. The PID service offers consumers and companies the opportunity to check their software, free of charge, if they are not sure whether it is original software or not. Since this service was launched in 1999, Microsoft has been able to check over 240,000 sent-in or seized products for genuineness. An examination of such products revealed 96 percent were illegal. The sender usually receives information on the genuineness of the product within 24 hours of it being received by Microsoft. "Consumers and companies who have purchased unlicensed software expose themselves, sometimes knowingly, sometimes unknowingly, to the risk that they may be prosecuted under civil or even criminal law for this illegal use, by the respective owner of the rights to the product. This can lead to claims for damages and costly court proceedings," explains Dr. Swantje Richters, attorney at Microsoft Deutschland GmbH.

Sources: Microsoft, OpSec

Events

Global Secure Summit

February 4-7, 2010 London, England

OpSec is presenting at this event. For more information, please visit www.globalsecuresummit.com

International Toy Fair Nuremberg

February 4-9, 2010 Nuremberg, Germany

OpSec is attending this event. For more information, please visit www.spielwarenmesse.de

American International Toy Fair

February 14-17, 2010 New York City

OpSec is attending this event. For more information, please visit www.toyassociation.org

ISPO Winter

February 7-10, 2010 Munich, Germany

OpSec is attending this event. For more information, please visit www.ispo.com

CEBIT 2010

March 3-8, 2010 Hannover, Germany

OpSec is attending this event. For more information, please visit www.cebit.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
Marketing Director
Email: tmock@opsecsecurity.com



©2009 OpSec Security, Inc.

