



Brand Alliance Insights

February 2009

Hello AGMA Members and Associates:

Welcome to Brand Alliance Insights! AGMA held its Annual Meeting of Members and first conference for 2009 at Cisco's headquarters in San Jose on January 21 and 22. In this issue of Brand Alliance Insights, we will recapture highlights from the many outstanding presentations that were given. Topics ranged from the challenges that the Internet presents to brand owners, tools for implementing better policies and processes for channel reporting and audits; the effects of counterfeit products on U.S. infrastructure, manufacturers, distributors and consumers; and partnering with law enforcement agencies to ensure successful litigation

Special thanks to Cisco for providing a perfect venue to kick off AGMA's 2009 conferences.

Welcome by Phil Roush VP Finance, Cisco

Mr. Phil Roush is a visionary that drives and nurtures Cisco's strategy and actions combating gray market and service fraud. He could not "hide" his passion for this subject while also testing the audience about AGMA's history and also sharing some very interesting insights into Cisco successes in curbing gray market and service fraud.

Stolen Identities used to Defraud Partners

Stolen corporate and identity information is being used to defraud resellers of computer and network equipment. Purchases are being made with what appears to be legitimate company identity and credit information, however, the ship to locations are not related to the end customer. The reseller has then been unable to collect payment from the end customer, who turns out to be a victim of identity theft.

Now more than ever, diligence is required in verifying end-customer identity, shipping and credit information. Pay extra attention to the end customer's Ship To address if it differs from the end customer's Bill To address.

How to Bring a Case for Prosecution to a U.S. Attorney's Office?

Fortunately Richard Cheng, Assistant U.S. Attorney provided four top answers:

1. Be honest, reasonable and logical when dealing with the government. Tell them what happened, who is suspect, detail what was taken, cost of goods, internal and external procedures for tracking and why handled accordingly, etc.
2. Follow the money and ensure traceability.
3. Help the attorney(s) understand your company's operations, how records are maintained, what records are available, who handles the records, etc.
4. Juries understand customer service; thus, always be "customer service" oriented.

The United States Attorney General's Computer Hacking and Intellectual Property Units employ approximately 230 attorneys specializing in intellectual property. The CHIP offices currently receive cooperation with 49 countries which provide immediate assistance in numerous capacities.

Final emphasis, be persistent when contacting their offices and build relationships!

Richard C. Cheng, Assistant U. S. Attorney for the Northern District of California
Computer Hacking and Intellectual Property Unit at (408) 535-5032
richard.cheng@usdoj.gov

Channel Compliance and Partner Audits

Hitachi Global Storage Technologies' Jim Vanlandingham detailed an overview to develop a channel partner audit program including the creation of a channel reporting and gray market policy, which HGST incorporated into its distribution contracts for all new channel partners. Not surprisingly "audit" generated a lot of audience participation during this presentation!

Jim stated that in implementing a partner audit program, it's best to begin by defining gray marketing and the importance of timely and accurate POS reporting, outlining financial penalties for violations. As you begin your program, consult with your internal departments (i.e. global sales, legal, pricing), schedule regional audits, and begin audits quickly after the audit announcement letter is sent. Anne Kiernan, Vice President, Worldwide Sales Operations for HGST added after the audit is completed she recommended you document problem areas, provide the channel partner specific corrective actions and timelines for implementation, and finally attach these agreed to corrective actions as an addendum to the contract. Additionally, it is important to follow up to ensure channel partners have implemented the corrective actions by the agreed to dates.

Go after the bad or the questionable! Hitachi GST has found that most channel partners understand the importance of the audit program.

Anne Kiernan, Vice President, Worldwide Sales Operations
anne.kiernan@hitachigst.com

Jim Vanlandingham, Worldwide Channel Compliance Manager
James.Vanlandingham@hitachigst.com

Law and Best Practices

Two of Northern California's best IP litigators Jeff Hallam and Rick Nelson from Sideman & Bancroft shared insight on proving *knowledge* in counterfeit, discount fraud, and service abuse criminal prosecutions. A key element is *knowledge*, i.e. being able to prove that the alleged criminal *knowingly* engaged in a scheme to defraud; "when" was the law broken and how can the government prove that the criminal knew that his representations were false, or that he was knowingly trafficking in counterfeit products? Additional tips - You should always make sure that the key provisions in your contracts, service agreements, website agreements, etc. are "readily seen and not buried in small print". Make sure you can track and trace your follow-ups calls, correspondence, etc. with the suspect, and always have proof of delivery for all cease and desist letters. Jeff and Rick highly recommend you have a policy in place to enforce contractual obligations with channel partners (including decertifications where appropriate); communicate with partners on a regular basis, obtain end users signatures accepting terms and conditions, and always document a transaction.

Jeff Hallam at jhallam@sideman.com
Rick Nelson at rnelson@sideman.com

Tipping Points and the Internet Ecosystem

Keeping with the theme of the day, Michael Kiefer with BrandProtect reemphasized the necessity of some active programs dealing with gray market fraud and counterfeiting corporations must establish and good internal controls. The first order of business is to have executive buy in, followed by corporate short and long investment to produce a positive return on investment, creating policies and procedures, etc. Michael provided shocking case studies covering internet abuses and shared his Enterprise Internet Risk Mitigation as a best practice tool. Gartner predicts that by the end of 2010, criminals will routinely use the Internet to extort funds from organizations, threatening to damage their

corporate reputation by ensuring that routine online search requests will return negative or even libelous results.

Michael Kiefer at mkiefer@BrandProtect.com

Microsoft Initiatives

What's the cost for global IT counterfeiting? How difficult is it to prosecute and successfully win counterfeit cases? Both are getting better with implemented programs, policies and tracking systems set in place to thwart the unscrupulous. Technology contributes to economic development and foreign governments want to attract companies to their countries; therefore, have your compliance in tact and not optional with your channel partners. It's imperative to: Educate and engage customers on value of genuine and the risks of counterfeit. Engineering continue develop innovative products with safeguards and anti-counterfeiting technologies and features hence more value for genuine user, make piracy harder and to protect customers and partners. Enforcement and collaborate for standards, policies, regulations, compliance and legal actions.

Cori Hartje at corih@microsoft.com

Public Policy Update

AGMA submitted a comment letter to the General Services Administration supporting the proposal to amend Federal Acquisition Regulations to require the government to procure IT products through authorized distribution channels and to require vendors to certify as to the authenticity of the products they sell. To review the comment letters, please visit www.regulations.gov.

The House of Representatives reintroduced a trade enforcement bill which would, among other things, create new IP enforcement leadership positions at Treasury, CBP and ICE; accelerate adoption of border risk assessment modeling techniques; limit mitigation of civil fines and improves their collection and enhance training of foreign border officials.

The negotiations over the Anti-Counterfeiting Trade Agreement continued in Paris last December. Discussions covered order enforcement, civil enforcement, international cooperation/enforcement practices and criminal enforcement. Negotiators also took up the topic of Internet issues for the first time and ways to make the ACTA process as transparent as possible going forward without compromising the negotiations.

Bob Kruger: bobkruger@verizon.net

Counterfeit and the Industrial Base

AGMA asked Teresa Telesco with the Bureau of Industry and Security for an encore after participating in last October's conference. The BIS mission is to advance U.S. national security, foreign policy and economic interests. It develops export control policies, issues export licenses, prosecutes violators, as well as monitors the capabilities of the defense industrial base. BIS is currently assessing the impact of counterfeit electronics on U.S. supply chain integrity, critical infrastructure, and industrial capabilities. BIS's final report will recommend best practices to mitigate risk to U.S. supply chain.

Ms. Telesco's presentation covered such topics as the pervasiveness of the problem, the types of counterfeit products that are uncovered, how counterfeits are detected and where they come from, why counterfeits enter the supply chain, the efficacy of testing for counterfeits, steps taken after discovery of counterfeits and recommended best practices.

The completed report is due out May 2009. If you would like a copy of the presentation, please contact Joanne Cooke at jcooke@agmaglobal.org.

Teresa Telesco, Industrial Analyst of BIS: ttelesco@bis.doc.gov

Customs Interdiction Program

What is the Customs and Border Protection role in intellectual property enforcement? Primarily seizure and forfeiture – anti-counterfeiting operations. The CBP also provides training programs throughout the US, Europe, China, India in areas of risk management, identification and enforcement. Working with IP owners to determine what risk they face from infringing imports, then implementing measures to address the risk. Primarily through seizure and their focus is generally on imports.

The first order of business for IP owners is to have the trademarks recorded with the U.S. CBP for a minimal cost of ~\$190. You may contact the CBP help desk at (562) 980-3119 Ext. 252 or www.cbp.gov. Consider posting your training manuals on the CBP secure website which will an important tool to properly identifying your IP.

Mark Goins at mark.goins@dhs.gov

Pioneering Authentication Solutions for a Challenging World

With more than 20 years of authentication experience, LSA executives presented a case study that exemplified their philosophy of providing cost efficient, seamless brand protection, anti-counterfeiting solutions that restore brand confidence and protect corporate profits. Their resourceful custom solutions can minimize the impact of authentication integration and hold down implementation costs. Also, whenever possible, they strive to create “green” solutions.

For additional information, please feel free to contact Richard Zucker at rzucker@lsauthentication.com or Gary Gray at ggray@lsauthentication.com



Executive Briefing Center!

Cisco generously hosted a tour of its amazing Executive Briefing Center. Guests took a glance at the future of high technology and how it is revolutionizing the way global business is conducted. Thank you Cisco for the opportunity to peruse your highly informative venue!

For tour information please contact Mercedes Thompson at (408) 526-4711

Announcements

AGMA elected the following directors Phyllis Massey, Ram Manchi, Peter Hlavnicka, Franziska Hanreich, and Chris LaChapelle. Cori Hartje with Microsoft was also elected and will also become a new director effective March 1st.

If you would like additional information on any of the presentations above or membership details, please contact Joanne Cooke, Executive Director at (510) 400-8747 or by email, jcooke@agmaglobal.org. We look forward to seeing everyone at the next AGMA conference in Hong Kong on March 12th or in Houston April 15-16 with host at Hewlett-Packard.