Assessing the Risk and Impact of Counterfeit Electronic Products

Brian Monks, Ovidiu Munteanu, Noe P. Navarro
Underwriters Laboratories, Inc., Northbrook, IL

Abstract
Counterfeiting is a widespread problem that affects every industry and which has the potential to significantly erode a company's bottom line. According to the International Anti-Counterfeiting Coalition (IACC), the global trade in counterfeit products has increased from $5.5 billion in 1982 to approximately $600 billion annually today. In the U.S. alone, counterfeit goods cost businesses between $200 billion to $250 billion annually [1].

The impact of counterfeit products is not just about tangible financial losses. Counterfeit products can negatively impact a company's brand, reputation and perceived commitment to quality. Because counterfeit products can also expose consumers to potential safety hazards, their availability may carry legal ramifications for companies.

The good news is that companies can assess the risk of being targeted by counterfeiters, and can implement a plan to protect against such risks. By following the appropriate steps, companies can determine how to protect their physical and intellectual property assets, identify the elements of an anti-counterfeiting program and implement an anti-counterfeiting plan. However, any anti-counterfeiting plan must be tailored to a specific company's needs, based on size of the company, the type of products, the complexity of the supply chain and the markets in which the company does business.

Many companies have taken rigorous steps to protect their intellectual property, the quality of their products and their reputation in the marketplace. These steps include the introduction of holographic labels, the use of special color schemes to identify specific product types and the application of overt and covert security coding. In addition, a number of companies have partnered with customs officials in anti-counterfeiting efforts, resulting in the seizure of millions of counterfeit products, including electronic products.

Introduction
In May 2009, the U.S. Department of Justice revealed the details of an international investigation known as Operation Network Rider. The investigation involved counterfeit Cisco networking devices manufactured in China and procured via the Internet, with an estimated value of $143 million. Had these devices been intended solely for use in typical business network operations, the discovery might not have been so alarming. However, the U.S. General Services Administration had authorized the purchase of 200 Cisco Gigabit Interface Converters, to be delivered to a Marine Corps base in Iraq near the hot zone of Fallujah [2] and these counterfeit devices somehow made it through the Pentagon's rigorous procurement process.

Fortunately for the troops in Iraq, the counterfeit networking devices were intercepted before being installed in the field, thereby avoiding potentially life-threatening consequences. But examples such as these occur on a daily basis, both in military procurement and in normal commercial operations. What's worse, many manufacturers may not even be aware that they have a potential problem with counterfeit products.

The problem of counterfeit electronic devices is not an isolated problem, but a part of a massive global trade in counterfeit products. According to the Counterfeiting Intelligence Bureau (CIB), counterfeiting accounts for between 5 percent and 7 percent of world trade [3]. This statistic suggests that any company involved in global trade is susceptible to eventually being caught in a counterfeiting net.

Counterfeiting presents several potential problems for companies. First, counterfeiting is a crime that threatens economic growth and can stifle innovation. If a product or group of products is considered to be unsafe or unreliable because of the widespread availability of counterfeit alternatives, it can create a negative perception for an entire industry. Second, counterfeit products can adversely affect a company's brand reputation. A brand that is directly or indirectly associated with products offering poor reliability can be detrimental to the company's overall reputation. Finally, there are legal ramifications to consider. If a counterfeit product bearing the company's brand name results in safety concerns that lead to a fire or injuries, the company could become the target of legal action.

In the end, legitimate companies have the most to lose from counterfeit products. That's why companies should take steps to combat the counterfeiting of their own products by assessing the potential problem and implementing anti-counterfeiting measures. It is also a good strategy to work with other manufacturers within the same industry and in other industries, and with anti-counterfeiting agencies, to develop solutions.

Assessing the Situation

Risk Analysis

Despite widespread counterfeiting activities, many companies may be unaware that they have a problem. Therefore, it's important to analyze the risks that exist within a given industry, and with certain types of products. For example, low-cost products that are sold in large numbers and which can be easily copied are frequent targets for counterfeiters. Similarly, counterfeiters also focus on expensive products with high-profit potential.

New items that are in heavy demand are also high on counterfeiters' hit lists. For example, each new generation of a popular video game console typically results in a new round of counterfeit games and accessories that flood the market. The supply chain is also an important cog in the counterfeiting machine. The less control a company has over the network of suppliers and distributors, the greater the opportunities for counterfeit products to enter the supply chain.

Here is a list of the key factors that present the greatest counterfeiting risks:

- ***High-volume, low-cost products:*** Such products are easy to produce on a mass scale.
- ***Products in high demand:*** A product that's in demand will attract the attention of counterfeiters because of the profit opportunity it presents.
- ***Products with large market share:*** Being at or near the top of the industry means success. Unfortunately, it also means being the target for counterfeiters. If customers are looking for a top brand name, counterfeiters will see a great opportunity.
- ***Products that lack security features:*** Security features, such as holographic labels or custom colors, can deter counterfeiters by making phony products difficult to replicate and fake products easier to identify. Products without such security features are easier to counterfeit.
- ***Complex, loosely-controlled supply and distribution chains:*** The more extensive the supply or distribution chain, the more challenging it becomes to track a product's development.
- ***Purchasing components and materials based on price alone:*** Counterfeiters don't just target end products, but also product components. Low-priced components may be attractive to legitimate manufacturers, but counterfeit components present the same risks as counterfeit finished products.
- ***Selling products on the Internet:*** Selling products online potentially means a loss of control over distribution, making it easier for counterfeiters to sell knockoffs of products without the manufacturer's knowledge.

Constant Communication

Constant communication is another key in determining whether a company has a counterfeiting problem. Companies must be continuously aware of activities in their marketplace, and ask questions of key people throughout the product chain, from sales to distribution to retail outlets.

For starters, the sales force can be a valuable resource in detecting suspicious activity. For example, if the returns department has been consistently receiving defective products, the company may want to evaluate those products to determine their legitimacy. If a product is not authentic, there may be an opportunity to gather valuable information from the party that returned it.

Similarly, the engineering department should regularly communicate with sales, marketing and other company departments to advise of changes to a product's configuration. Providing the entire distribution network with timely access to this information will allow all key departments to distinguish between legitimate and counterfeit products. The company should also pay close attention to marketplace anomalies, such as selling prices that are excessively low.

Companies should also consider conducting market surveillance in geographic areas where there are anomalies in market share. Low market share could signal penetration of counterfeit products. Alternatively, some companies have found that their products hold leadership positions in markets they haven't entered, due to the sale of counterfeit versions of those products.

Full Team Effort

Anti-counterfeiting isn't just about making tangible efforts to protect intellectual property. It's also about demonstrating a corporate-wide commitment to take the threat of product counterfeiting seriously. That's why anti-counterfeiting efforts must be a top-down undertaking, requiring the active involvement of the company's senior management to ensure that all departments get the message. Without active engagement and support from a company's senior executives, individual company departments may find it difficult to get their anti-counterfeiting efforts off the ground.

Aside from the involvement of a company's top executives, the purchasing department must make sure the components it procures are not counterfeit. Procuring parts on the basis of price alone can unnecessarily expose a company to counterfeit components, since an unusually low price may be an indication that a component is not legitimate. And counterfeit components in an otherwise legitimate finished product will expose a company to the same risks as a completely counterfeit product.

A reasonable approach to avoiding counterfeit components is to purchase components through franchised distributors and the franchised aftermarket [4]. Distributors should be expected to provide the documentation necessary to trace the origins of the parts they sell. If such documentation is not available, buyers should demand other evidence that can identify the manufacturing source. A supplier's inability to provide proof of legitimate component production is a potential indication that the components involved are counterfeit [5].

A company's anti-counterfeiting efforts also extends to the legal and human resources departments, who are responsible for ensuring that all employees have executed appropriate non-compete and non-disclosure agreements. A company's legal department also has the responsibility to protect the company's intellectual property assets, including taking the necessary steps to ensure the prompt registration of a company's patents and trademarks with the U.S. Patent and Trademark Office. A company that fails to diligently protect its intellectual property may be at a significant disadvantage in subsequent efforts to defend that property in prosecuting counterfeiters.

Protecting Your Assets

Along with marshaling resources throughout the organization, there are several logistical steps that companies can take to protect their intellectual assets from counterfeiters. In addition to registering intellectual property, companies should also record their registered marks with the U.S. Customs and Border Protection. This step helps to protect intellectual property at all ports of entry in the United States, and can help to block the importation of counterfeit products at the borders.

It's also recommended that companies record or register their intellectual property in every country in which they conduct business, even if overseas production is several years in the future. Many countries follow the "first to file" rule, granting intellectual property rights to the first person or organization registering a corporate name or trademark. In some cases, companies have attempted to register their intellectual property in a new market, only to find that a counterfeiter had beaten them to it.

Elements of an Anti-Counterfeiting Program

End-to-End Security

Manufacturers who discover that their legitimate products are being counterfeited are sometimes reluctant to come forward with the information, in the belief that admitting to a counterfeit problem will adversely affect their reputations. But counterfeiting affects virtually every industry in the world and the problem will not resolve itself without the proactive involvement of all manufacturers. Even companies who are not currently dealing with a counterfeiting problem can reduce their risk by establishing a comprehensive anti-counterfeiting program.

For starters, every manufacturer should integrate security features into their products. There are product security features that are reasonable and appropriate for every industry, product and price point. One size certainly does not fit all, but there are viable solutions for every situation, from holographic labels and radio frequency identification (RFID) tracking, to authentication features incorporated into packaging materials, labels or inks.

Companies must also make sure that their entire supply chain actively participates in their anti-counterfeiting efforts. Even if a manufacturer of finished products implements anti-counterfeiting measures at the product level, it can still be vulnerable to counterfeit components from suppliers. Manufacturers should increase security throughout the supply chain using appropriate security features to authenticate products.

As noted previously, it's equally important to know the source of product components. That means working only with reputable suppliers and distributors, developing strong relationships with them, and implementing reporting systems that allows suppliers to provide information through the supply the chain whenever they detect suspicious activity [6]. Although frequently switching suppliers may lead to cost savings, it can also introduce unknown vendors into the supply chain that can put a company at risk.

Finally, companies need to perform due diligence checks at every stage of their products' lives, including assembly, packaging, distribution and disposal. These checks should also include the proper management of waste produced during the manufacturing process. Counterfeiters often re-create products from scrap, which is why security should be part of the waste management process as well.

Make the Right Contacts

Regardless of the degree of vigilance at the company level, an anti-counterfeiting program cannot function effectively in a vacuum. That's why a large part of an effective anti-counterfeiting program involves working with Customs and Border Protection authorities and with global law enforcement agencies. For example, providing training to enforcement agencies, including product identification manuals and information on security features, will make it easier for officials to distinguish between genuine and counterfeit products. Working with customs and law enforcement also means committing the necessary resources to support these officials at all times. This may involve establishing a dedicated hot line or secure Website for law enforcement officials, so that they can access critical product information when necessary.

It's also important to forge strong partnerships with other anti-counterfeiting resources, especially in those instances where products are manufactured across borders. Increasing awareness efforts and legislative activities will also help put the issue at the forefront of agencies that can take concrete action. Other measures companies can take include:

- Educating distributors and other stakeholders;
- Moving intellectual property protection onto the agenda of trade associations;
- Joining intellectual property protection coalitions and associations;
- Sharing best practices with other manufacturers to help protect the industry.

When collaborating with other manufacturers, it's important to work with organizations from different industries. Counterfeiters don't often observe industry boundaries and today's purveyor of fake pharmaceuticals could be tomorrow's dealer of phony printed circuit boards. Counterfeiting affects everyone, so it's in a company's best interest to help put away counterfeiters of all stripes.

Because intellectual property abuse often originates internally, companies should conduct background checks on potential hires in key departments, such as engineering, purchasing and production. Companies should also consider establishing a confidentiality policy, and require all employees and suppliers (including contractual partners and vendors) to sign it. Intellectual property leaks can also occur after an employee leaves the company, so a non-disclosure or non-compete agreement lets employees know that they are legally bound not to disclose intellectual property information, even after their employment ends. Such polices and agreements should receive proper legal review to ensure that they are enforceable under local, state and federal laws in the regions where the company operates.

Implementing the Plan

The implementation of a company anti-counterfeiting plan must be tailored to an organization's needs and based on several factors. For example, the number of company employees will often dictate the approach that should be taken regarding implementation. An organization with 100 employees will have a different set of requirements than a company with 20,000 employees. Likewise, a company that produces one or two high-demand products will have different needs than a manufacturer producing popular items in several different product categories.

Companies must also consider the various geographic locations where they do business. The location of suppliers and distributors is an important consideration in determining how an anti-counterfeiting program should be approached. If the supply chain extends across multiple countries, companies must also consider applicable laws and regulations in those regions.

A manufacturer may choose to implement an anti-counterfeiting program on its own, but there is no "off-the-shelf" solution that can address each organization's unique requirements. Because the implementation of an anti-counterfeiting program is a complex undertaking that involves a significant commitment of resources, manufacturers often have difficulty knowing where to begin. Guidance from an independent third party with expertise in developing anti-counterfeiting programs and with strong relationships with global law enforcement authorities can help put manufacturers on the right track.

Underwriters Laboratories works with local, national and international law enforcement agencies to identify and seize counterfeit products. Since 1995, U.S. Customs and Border Protection has seized more than $150 million of products bearing counterfeit UL certification Marks. UL has trained thousands of law enforcement authorities to identify and recognize legitimate UL certification Marks, and invests about $2 million annually in anti-counterfeiting activities. UL also works with governments and international enforcement agencies including Interpol, Europol, the Royal Canadian Mounted Police and the World Customs Organization, to thwart counterfeiting and to help stop the flow of counterfeit goods. Finally, UL's active participation in U.S. legislative efforts helped get the "Stop Counterfeiting in Manufactured Goods Act" signed into law in early 2006.

Although no single source can provide all the answers, asking a knowledgeable third-party resource the right questions can help bring clarity to the specific situation.

Zero Tolerance: The Only Approach

Counterfeiting is a serious crime that affects all industries, erodes companies' bottom lines and leaves the public exposed to significant reliability problems and potential safety hazards. That's why manufacturers must actively and aggressively work to combat counterfeiting. The benefit that individual companies derive from an anti-counterfeiting program depends on how much they are willing to invest in its success.

Manufacturers must take a zero tolerance approach to counterfeiting. It's not just a matter of getting individual counterfeit products off the shelves. It's everyone's responsibility to support law enforcement with whatever is required, up to and including testimony during prosecutions. Companies need a high level of commitment to have the necessary credibility to work effectively with law enforcement. By implementing a comprehensive anti-counterfeiting program, partnering with other organizations and working with the authorities, every company can help combat this worldwide problem.

Summary

The rapid increase in worldwide counterfeiting over the last few decades is definite cause for concern. Counterfeit products represent a significant cost for all parties in the supply chain, and unreliable, low-quality products can expose consumers to potential safety hazards, resulting in loss of revenue, brand value, and reputation, as well as exposure to investigations and legal actions. However, companies can assess the risk of being targeted by counterfeiters, and can take rigorous steps to protect against such risks. Risk assessment includes analyzing the industry, the products, the product demand, and the product distribution channels. Risk mitigation involves a plan that incorporates a good communication strategy, a controlled distribution network, integrated security features, and collaboration with customs and border authorities. Ultimately, there is no off-the-shelf plan that can guarantee 100% positive results for all manufacturers. But, given the prevalence of global counterfeit trade, having no plan presents too great a risk.

REFERENCES

[1] IACC (International Anticounterfeiting Coalition), About Anticounterfeiting, http://www.iacc.org/about-counterfeiting/

[2] Wright, Rob, "Cisco Counterfeiting On the Rise", CRN, Aug 4, 2009

[3] ICC Commercial Crime Services, Counterfeiting Intelligence Bureau, http://www.icc-ccs.org/index.php?option=com_content&view=article&id=29&Itemid=39

[4] Wilson, John P., "Guidelines for Avoiding Counterfeit Components", L3 Interstate Electronics, 2010, pp 4

[5] Keller, John, "The scourge of high tech", Military and Aerospace, July 1, 2007

[6] Livingston, Henry, "Avoiding Counterfeit Electronic Components", IEEE Transactions, Vol 30, No. 1, March 2007, pp 187-189

Assessing the Risk and Impact of Counterfeit Electronic Products

Brian Monks

Vice President, Anti-Counterfeiting Operations

Underwriters Laboratories, Inc.

The UL Certification Mark

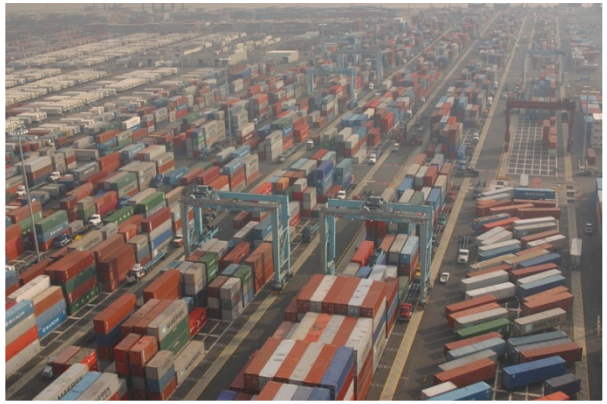
- What it is…
- A declaration that UL has tested and evaluated representative samples of that product and determined that they meet UL requirements
- Evidence of follow-up agreements between the manufacturer and UL
- A voluntary Mark

- What it isn't…
- An approval
- An endorsement
- A warranty
- Legally mandated

UL by the Numbers - 2009

- 20 billion UL Marks appeared on products
- 66,149 manufacturers produced UL certified products
- 89,994 product evaluations were conducted by UL
- 570,088 Follow-Up Services inspections conducted
- 19,597 types of products were evaluated by UL
- 120 UL inspection centers in service
- 102 countries with UL customers
- 1,420 current Standards for Safety published by UL
- 68 laboratory, testing and certification facilities
- 6,921 employees in the UL family of companies

UL’s Anti-Counterfeiting Operations (ACO)



How We Got Started

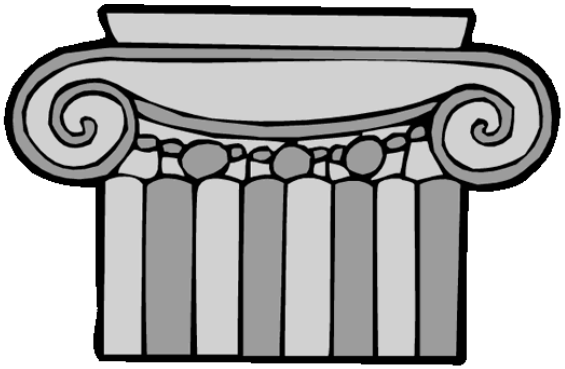
- Program now in its sixteenth year
- A UL Client complained of competitor selling products at a suspiciously low price point
- Counterfeit UL Mark was verified
- Prompted our first call to US Customs
- Recorded Marks with US Customs
- Most commonly counterfeited goods tend to be low-cost, high volume products – extension cords, power taps, adapters, etc.
- Introduced holographic labels for “high-risk” categories
- Learned that dedicated staff and resources are required for success

Our Mission

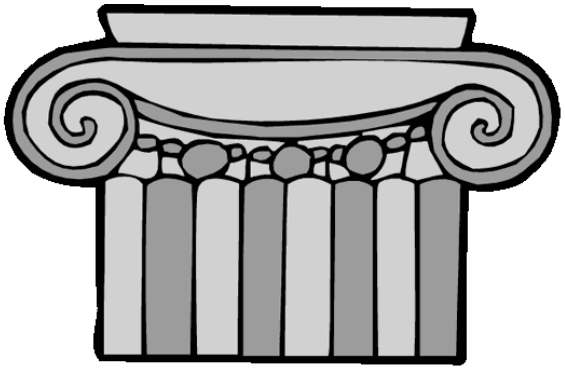
1) To preserve and enhance the integrity of the UL family of Marks
2) To protect the safety of consumers around the world from the potential hazards associated with goods bearing counterfeit UL Marks
3) To provide additional value to our customers who have invested the time and resources to meet UL's safety standards

UL’s ACO Program

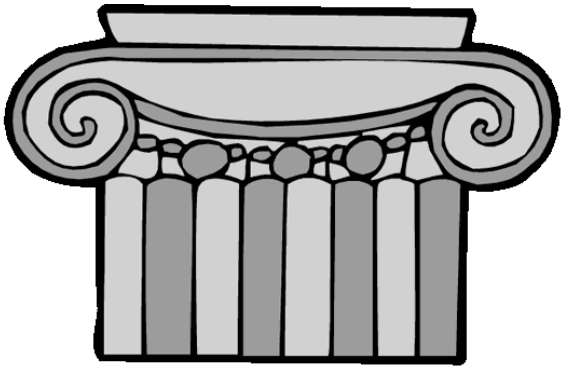
ENFORCEMENT



EDUCATION



PARTNERSHIPS



Enforcement

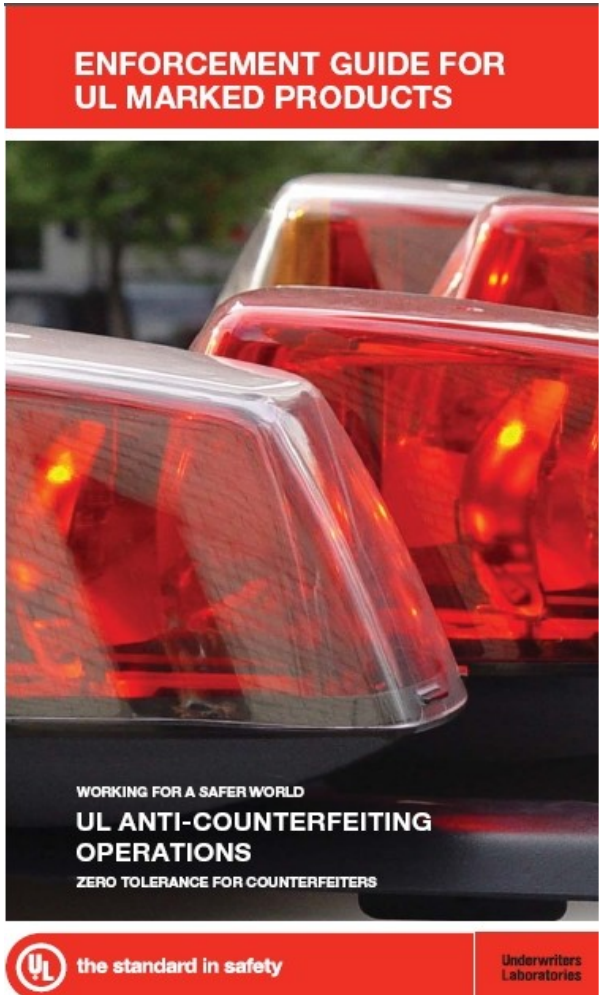
Zero Tolerance Policy

It is the policy of Underwriters Laboratories Inc. (UL) not to consent to the importation, exportation, or manipulation of merchandise that has been seized by U.S. Customs or any other law enforcement agency for bearing counterfeit UL Certification Marks.

This policy is uniformly applied and is considered reasonable and necessary in order to protect the integrity of UL's Registered Marks.

UL does not compromise or negotiate with respect to this policy.

UL's Commitment to Law Enforcement



- A timely response to all inquiries;
- Complete and full product analysis, professional reports and timely disclosure
- On-site authentication of UL-Marked products as required by law enforcement during the execution of warrants
- UL testimony as needed at all judicial proceedings
- Certification Mark registration certificates
- Victim impact statements

Customs and Border Protection

- CBP focus on products posing health and safety threats
- CBP training remains a core objective
- CBP seizures of counterfeit UL-marked goods increased 100% over 2009 YTD
- “Need for Speed” – limited window for law enforcement to detain products

Investigations

- Intelligence-led investigations
- Law enforcement agencies from around the world
- Leads from seizures, consumer/ customer reports, market surveillance

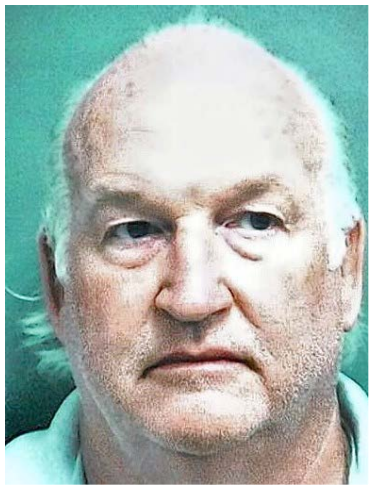
SunSentinel.com | ARTICLE COLLECTIONS

Owner of Boca Sign Shop Arrested for printing fake safety labels. Police say: Signsations owner Jack Glover, 58, arrested on 34 counts of counterfeiting and one count of organized fraud.


4) 893 Palmetto East Park Rd. Boca Raton

Here is an "Ice Cream" store sign just installed in last mth. The pics speak for them selves.

SIGNSATIONS



“Glover said he made the labels because he knew they were needed to get permits and thought the signs met safety standards, the report said.

He is accused of printing fake Underwriters Laboratories labels and placing them on 34 electronic signs installed at South Florida businesses. The labels led customers and city officials to believe the signs met the safety standards of the nonprofit testing organization, the report said.

Underwriters Laboratories inspectors contacted authorities after learning in December that Signsations was illegally using its logo, police said.

Glover is being held at the Palm Beach County Main Jail in lieu of $25,000 bail.”

Our Work in China

- Ongoing training for HK and China Customs
- Local counsel and security firms a necessity
- 50+investigations undertaken 2010 YTD
- Successful AIC actions resulted

Education – Law Enforcement

- Training for US Customs and Border Protection personnel
- Training for Immigration and Customs Enforcement personnel
- Training for other federal and local agencies (FBI, DOJ, USPTO, local police, Fire Marshals, etc.)
- Training for international authorities (police agencies, INTERPOL, Customs, etc.)

Education – Outreach

- Membership in anti-counterfeiting industry organizations and task forces
- Provide testimony to US Senate and Canadian Parliamentary Committees
- Primary sponsor and organizer of the International Law Enforcement IP Crime Conference – 2007-2010
- Participation as keynote speakers and/or panelists at industry events

Partnerships

U.S. Customs and Border Protection

U.S. Immigration and Customs Enforcement

Technology

- **Gold background to help U.S. Customs officers and other law enforcement agencies, distributors, retailers and consumers quickly identify the new label**
- **Color shifting ink similar to that in the new U.S. paper currency**
- **Repeating pattern of floating UL symbols, a distinctive burst pattern around one of the floating UL symbols, detailed micro-printing and wavy lines**