KPMG

ELECTRONICS, SOFTWARE & SERVICES

Managing the Risks of Counterfeiting in the Information Technology Industry

INFORMATION, COMMUNICATIONS & ENTERTAINMENT

AUDIT ▪ TAX ▪ ADVISORY

Contents

Executive Summary

Counterfeiting is among the most challenging issues facing the information technology (IT) industry today. Illegal replicas of brand-name high tech products are flooding the marketplace, cutting into legitimate companies' revenue and reducing their ability to invest in research and development (R&D). Proliferation of technology used to make computers, servers, and a host of high tech products—as well as a lack of regulatory enforcement in developing nations—is accelerating counterfeiting. It is now estimated that as much as 10 percent of all high tech products sold globally are counterfeit.

The sight of street-corner vendors selling bootlegged CDs, DVDs, apparel, and jewelry is commonplace—and now counterfeit high tech products are becoming widely replicated by illicit producers and sold over the Internet. The public, however, is becoming more aware of the dangers posed by counterfeiting and the criminal organizations behind it, and many people are fighting back. Reports of connections between counterfeiters and terrorist organizations—and speculation that revenue generated by counterfeiters is helping to fund terrorism—have helped spur increased resistance.

Still, some governments are not devoting sufficient resources to help curtail counterfeiting activities, which generate billions of dollars each year in illegal revenue. As a result, industry associations and legitimate governments are teaming with law enforcement agencies to put pressure on egregious offenders and stem the flow of counterfeit products. Some IT companies are also conducting independent investigations, and the industry as a whole is working in concert with authorities to root out and prosecute offenders within their home countries.

Through heightened awareness of early warning signs—and increased vigilance in identifying and punishing both the manufacturers and distributors of counterfeit goods—progress is being made. But a coordinated, comprehensive program targeting the sale and distribution of counterfeit high tech products is necessary to protect consumers from poor quality goods as well as help secure the future of the IT industry.

KPMG LLP and the Alliance for Gray Market and Counterfeit Abatement (AGMA) conducted a study to help IT executives better understand the risks introduced by counterfeiting—and the steps that can be taken to help mitigate that risk. This white paper outlines the results of the study, which includes interviews with leading executives who provide insights to help safeguard brand-name products and reduce counterfeiters' ability to further harm the IT industry.

Most Profitable Criminal Venture

Despite IT products' sophisticated design and complex manufacturing, counterfeiting is a growing problem. As many as one in ten IT products sold may actually be counterfeit, according to interviews conducted with electronics industry executives. In some specific product cases the percentage of counterfeits may, in fact, be even higher (e.g., network interface cards). Conservatively estimated, this equates to about US$100 billion of global IT industry revenue that is lost to counterfeiters annually. Indeed, according to estimates by the International Chamber of Commerce, all counterfeit goods accounted for 6 percent of world trade in 2003, valued at a whopping US$456 billion.

KPMG LLP, the audit, tax, and advisory firm, in cooperation with the Alliance for Gray Market and Counterfeit Abatement, conducted a study to help IT executives better understand the causes of counterfeiting and its effects on IT customers, authorized distribution partners, and the IT industry overall.

"We found that counterfeiting and gray market channels often go hand-in-hand, so it's logical for AGMA to concern itself with both issues," says Marie Myers, AGMA president. "AGMA is dedicated to tackling the counterfeit challenge faced by our member companies and the potential harm counterfeiting causes to end customers and channel partners as well."

Most people still associate counterfeiting with currency, or a shady-looking man with a string of watches inside his lapel whispering, "Wanna buy a Rolex?" But people are becoming more conscious of the fact that counterfeiting is a much bigger problem. It poses a significant threat to leading companies in industries that form the basis of our global economy. By reducing revenue and harming brand equity, counterfeiting of IT and electronics products is eroding the integrity of the "supply and demand" business model.

Through research, we found that the most effective countermeasures to counterfeiting were driven from the top down into an organization by its senior-most executives. This suggests that, in the IT and electronics industries, it is important that the risks of counterfeiting be addressed at the highest levels of management. Each year, counterfeiters are siphoning off an increasing portion of the industries' revenue, so the time to act is now.

The shady man on the street is an obvious seller of counterfeits. Most people who buy a "Gucci" handbag from a street vendor for $10 know it is a fake when they buy it. So if the strap breaks the following week, they throw it in the trash and chide themselves for wasting $10. But an unwary online purchaser of a $2,500 computer may not be as understanding when it breaks, especially when he or she finds out that the product is not under warranty because it is counterfeit.

Unlike watches, motion picture DVDs, clothing, and music recordings, far more counterfeit IT items are hawked over the Internet than on street corners. Some of the largest distribution centers are trade markets in southern China that are supplied by nearby manufacturers. Rather than just mom-and-pop operations dealing in easily copied packaging, many counterfeit IT products are produced using high technology processes. As a result, the end product can run the gamut from a shoddy knock-off to a replica so well executed that even experts can be fooled.

"The U.S. Patent and Trademark Office says that 66 percent of the counterfeit goods seized at American borders now come from mainland China, up from 16 percent five years ago," reports *Fortune* magazine in its January 10, 2005, issue. According to *Fortune*—and pointing to the harm being wrought on China's technology entrepreneurs—Chinese companies are also beginning to seek governmental protection from counterfeiters within their own country's borders.

Many of the executives we interviewed believe that organized crime is involved in both the manufacture and distribution of counterfeit products of all kinds. Criminal factions, including terrorist groups, are suspected of using counterfeiting as a means of funding criminal enterprises or laundering money gained from nefarious activities. According to Harley Lewin, an attorney who has been pursuing counterfeiters in China for more than 20 years, counterfeiting "is the most profitable criminal venture."

Juan Zarate, the U.S. Department of the Treasury's assistant secretary for terrorist financing, agrees, saying terror groups became more sophisticated in funding their activities as the United States and other countries cracked down on money laundering through banks and other financial institutions. Counterfeiting is one of the methods used by terrorists to raise cash.

The price of an authentic product produced by a legitimate original equipment manufacturer (OEM) reflects the cost of research and development, brand development, manufacturing, marketing, and sales. By paying only the cost of manufacturing and sales, the counterfeiter is able to sell the counterfeit product below the price of the authentic one and make a significant profit.

For the company whose products are being counterfeited, the losses are doubly damaging. Counterfeits not only compete with authentic products for revenue, they can also harm a brand's marketplace equity, leaving the brand-holder with the problem of diminishing demand and rising product support costs.

The U.S. Patent and Trademark Office says that 66 percent of the counterfeit goods seized at American borders now come from mainland China.

— *Fortune* magazine

"Counterfeiting is one of the most significant threats to the free market," says Richard Girgenti, partner in charge of the KPMG Forensic[SM] practice. "It not only steals the value of intellectual capital, it stifles innovation and robs customers of the quality they expect from a brand."

Despite the difficulties involved in prosecuting counterfeiters across national boundaries with inconsistent laws, the economic benefits of making it more difficult for counterfeiters to copy and distribute IT products are clear.

Case in point: Acting on a tip received through the AGMA tip line, Hewlett-Packard moved fast to locate warehouses storing millions of dollars worth of counterfeit goods. Through surveillance, they traced the sales and supply chain in coordination with international law enforcement to locate the illegal manufacturing source. The case spanned two continents and five countries, resulting in the seizure of thousands of counterfeit IT products, closure of several "front" companies, and legal sanctions against entities in multiple countries involved in manufacture and distribution of counterfeits.

Lessons from Other Industries

The sale of counterfeit software and music CDs, movie DVDs, and, of course, high-end watches is widespread. The same is true of fashion sunglasses and popular-brand clothing and cosmetics. The common element in all of these cases is illegal use of a brand name—one that is well known and commands high prices. For the IT industry, the problem of counterfeiting is relatively recent. Therefore, we interviewed executives in industries where counterfeiting has been a long-standing problem—including pharmaceuticals, packaged goods, and motor vehicles—to learn from their experience.

The pharmaceuticals industry, for example, estimates that in some markets as much as half of certain products are counterfeit. That is cause for serious concern, not only because revenue and profits are being stolen but also due to threats to the health and safety of consumers.

In June 2004, Seoul, South Korea, police raided more than 100 pharmacies and seized large amounts of counterfeit Cialis® and Viagra®. These seizures were the result of a collaborative effort between the police and pharmaceuticals companies. Much of the initial investigation and efforts in building the case and tracking the counterfeiters was the result of work by the companies' own anticounterfeiting programs.

In 2003, South Korea imported US$1.1 billion in drugs. This, plus its proximity to China—a hub of counterfeit drug production—makes South Korea an attractive market for counterfeit drugs. But this is not an isolated example. According to drug industry estimates, in many developing countries up to 50 percent of available drugs are counterfeit; worldwide, the total is about 10 percent. India is also a problematic region for counterfeit drug production because the country only recently began to recognize the legality of patents.

Both IT and pharmaceuticals companies rely heavily on costly R&D for creating new products. Each manufactures products using expensive capital equipment and each invests heavily in global marketing and distribution. Research conducted by KPMG LLP and AGMA identified many similarities between IT and more mature industries regarding early warning signs of counterfeiting and the countermeasures being applied.

In many developing countries up to 50 percent of available drugs are counterfeit; worldwide, the total is about 10 percent.

Early Warning Signs

Counterfeiters do not announce their intention to copy branded products, and discovery often occurs by chance. But there are early indications that can signal when a company has a counterfeiting problem. We interviewed several professionals from high technology companies who are responsible for responding to counterfeiting. They identified the early warning signs described below.

Sudden Drop in Raw-Materials Orders

Many IT companies engage third-party contract manufacturers to produce their products. In some cases, component procurement is left entirely up to the contract manufacturer; in others, the OEM may procure them. In the OEM case, a sudden drop in raw-materials orders may be an early indicator of counterfeit part substitution. This is especially true if the volume of shipped devices is fairly constant. If a contractor is not buying the parts from the OEM, where are they coming from? If the contract manufacturer is not using authorized components, then products built using substitutes may be considered counterfeit. But in every case, use of unauthorized components risks compromising the end product's quality.

"Where high product quality benefits a company's brand, counterfeiting becomes a major assault on both brand and revenue," says Rich Rutledge, general manager of the PC components at Western Digital Corporation.

> Where high product quality benefits a company's brand, counterfeiting becomes a major assault on both brand and revenue.
>
> — Rich Rutledge, Western Digital Corporation

Increased Orders for Proprietary Components

In some cases, OEMs sell both manufactured goods and raw materials. For example, a maker of plug-in network interface cards based on its proprietary chip may also sell just those chips to motherboard providers who offer a built-in network interface. Obviously, the OEM has no way of really knowing if the chip it is selling will be used on the intended motherboard, or used to make counterfeit plug-in boards. Therefore, another warning sign is increasing volumes of orders for components without a commensurate increase in their legitimate target products.

Increased Grey-Market Availability

KPMG LLP's white paper *The Grey Market*, published in 2003, explains how legitimate products often flow through unauthorized channels. These grey-market channels can also facilitate distribution for counterfeiters. Grey-market distributors have no way of knowing how much product an OEM is making. Thus, they have no way of knowing whether sudden influxes of products into their channels are redirected legitimate OEM products or counterfeits. It is imperative for the OEM to pay close attention to the quantities of their products flowing through unauthorized channels. An upsurge may be a warning sign of counterfeits entering through those sales channels.

Increase in Service Returns

Most OEMs see the first tangible proof of counterfeiting when these units are sent back for service. The best copies may go undetected even by a technician, but other copies can be readily identified because of obvious differences in components or board layout. In general, OEMs know approximately how many products are likely to be returned for service. When there is a spike in returns, it may indicate either an OEM quality problem or counterfeiting.

Large Volume of Discounted Product Available

Many OEMs actively monitor marketplace pricing through Internet tools and other means, and can detect when large quantities of product become available on the open market at unusually low prices. These price indicators can signal counterfeits entering the marketplace.

China: A Favorable Environment for Counterfeiters

China attracts a huge influx of foreign direct investment (FDI) resulting in high technology capability with adopted know-how, accessible distribution in densely populated areas, and inconsistent regulatory enforcement. These factors—coupled with low wage rates, high unemployment, and a largely uneducated workforce—create a favorable setting for counterfeiting.

Whether it's computers, communications systems, drugs, or basketball shoes, most executives agree that southern China is a focal point of counterfeiting. "Every year 25 percent of our business is eaten away by counterfeits," according to Daniel Chow, former in-house legal counsel for a large multinational enterprise with significant investments in China and secretary for the China Anti-Counterfeiting Coalition, an ad hoc group of multinational enterprises with serious counterfeiting problems in China. In testimony before a subcommittee for Senate Governmental Affairs in April 2004, Chow said, "In terms of size, scope, and magnitude, trademark counterfeiting in China is considered by many to be the most serious counterfeiting problem in world history."

Chow, who is the Robert J. Nordstrom Designated Professor of Law at the Michael E. Moritz College of Law, The Ohio State University, added, "Brand owners in China estimate that 15 to 20 percent of all well-known brands in China are counterfeit and estimate their losses to be in the tens of billions of dollars."

Based on Chow's testimony, three key factors are the root causes of China's counterfeiting problem:

- Foreign direct investment with advanced technology
- Direct and indirect state support of counterfeiting, combined with protectionism
- Ineffective legal enforcement

FDI in China during 2003 was US$57 billion, according to the United Nations Conference on Trade and Development. Historically, the influx of FDI led to a concentration of legitimate, joint venture manufacturing in Fujian and Guangdong provinces. Not coincidentally, the bulk of Chinese counterfeit manufacturing is also centered there. Manufacturing processes of legitimate companies in these provinces could easily "migrate" to illegitimate factories nearby.

In China, large wholesale markets are common to densely populated areas with good access to transportation. These are known hubs of counterfeit distribution.

The third factor is ineffective laws and deterrents. China's wholesale markets are the aegis of local administrations of industry and commerce (AICs). The AICs create and regulate them—a classic case of conflict of interest. The AICs receive revenue from the booth owners in the wholesale market and, therefore, are reluctant to do anything to diminish their revenue base, such as enforcing national laws against distributing counterfeits.

China's government has passed laws to satisfy the concerns of its trading partners, but it lacks coordinated efforts between national and local authorities to quell blatant manufacturing, distribution, and sale of counterfeit product. "We conducted a raid on an aftermarket dealer in China," says Linda Heban, vice president and chief trademark counsel for Harley-Davidson. "Actually, we had the AIC conduct the raid. But the problem is, when you stop one, another pops up."

Recently, encouraging signs are emerging from the Chinese government that point to the realization that counterfeiting could hinder economic development in the country.

According to *China Daily*, China's recent release of the judicial interpretation on intellectual property rights (IPR) infringement criminal cases attests to the country's updated efforts to fight the crime. The 17-article interpretation, which took effect in December 2004, materializes the legal principles in the previous IPR-related laws.

The move fully demonstrates the country's determination to stamp out IPR-infringing crimes, which are costly not only to the victimized organizations and individuals but also to the country's overall investment and market environment. Rampant piracy, for example, will lead to less confidence in innovation and independent development of technology.

Encouraging signs are emerging from the Chinese government that point to the realization that counterfeiting could hinder economic development in the country.

Mitigating Pervasive Counterfeiting

"High technology companies intent on reducing counterfeiting have no single 'magic bullet' at their disposal," says Peter Hunt, director of supply chain, product, and brand security for Hewlett-Packard. "Successful resolution of the problem requires a multifaceted anticounterfeiting program, dedicated resources, and leadership from the top of the company."

The following list of anticounterfeiting tactics was identified by executives of leading high tech companies, and includes techniques, pioneered by more mature industries, that are now being adapted by leading electronics companies.

- Designing-in and employing copy-resistant and anticounterfeit technologies on all products
- Continually evaluating anticounterfeit technologies, including radio frequency identification (RFID), security labeling, and other packaging technologies and techniques
- Coordinating with U.S. and international organizations and trade alliances such as AGMA, the International AntiCounterfeiting Coalition, and U.S. Immigration and Customs Enforcement (ICE) on responding to counterfeiting issues
- Partnering with international law enforcement and customs agencies to research and monitor the traffic in counterfeit IT products, and pursuing infringers
- Developing and deploying anticounterfeit education and training programs for internal and external stakeholders, including end users, channel distribution partners, and service and sales employees
- Signing product distribution agreements that contain specific language to protect the brand, including provisions for auditing and enforcement
- Ongoing monitoring of distribution streams of counterfeit products, such as Internet brokers, direct sales, retail outlets, wholesalers, and Internet trade Web sites
- Taking enforcement action against counterfeiting and other illegal operations using civil and criminal remedies
- Creating an internal anticounterfeiting task force, including stakeholders from finance, sales, and service organizations from all "hot-spot" regions in the world
- Layering anticounterfeiting controls into product and packaging designs, as well as into manufacturing, sales, order processing, services, and warranty processes
- Deploying a robust communications plan targeted at specific audiences, including end users, channel distribution partners, third-party service providers, and the manufacturers and resellers of counterfeit products

> It is really a combination of efforts—some proactive and some reactive—constituting a prevention, detection, and response strategy, that is most effective in mitigating pervasive counterfeiting.
>
> —Richard Girgenti, KPMG Forensic

- Providing a simple means—such as through the AGMA tip line—by which suspected product, Web site, or other infringements can be reported—and responding to such reports
- Creating a global brand protection function to manage the anticounterfeiting program for the company

As Hewlett-Packard's Hunt explains, no single tactic would be effective, but the combination of many tactics, applied consistently, will eventually yield benefits.

"It is really a combination of efforts—some proactive and some reactive—constituting a prevention, detection, and response strategy that is most effective in mitigating pervasive counterfeiting," says KPMG's Girgenti. "It's the holistic approach, rather than single rifle shots, that is most likely to succeed," adds Hunt.

Following are additional tactics that can bolster a holistic prevention, detection, and response strategy.

Identifying Geographical "Hotspots"

There are common characteristics among countries where counterfeiting is likely to be a problem, including large populations, low skill levels with high unemployment, low labor rates, weak law enforcement, and low government intervention. Brazil, China, India, Malaysia, Paraguay, and former Eastern Bloc countries fit this profile.

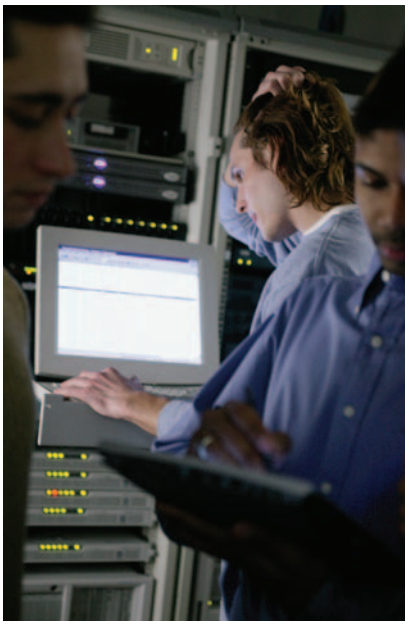
Make OEM Products Difficult to Copy

The second imperative is to make it difficult to copy legitimate products. In retrospect, the high tech industry first followed the mantra of "design for manufacturability." Later, as components became more complex, the mantra became "design for testability." Perhaps the industry needs a new mantra: "Design to prevent counterfeiting."

Better Monitoring and Auditing of Contractors, Supply Chain, and Distributors

Nearly all interviewees agreed that contract manufacturing poses greater counterfeiting risks than internal manufacturing. More stringent contracts and auditing, however, can help reduce the risk. They enhance both prevention and detection, and they spell out specific remediation plans. It's also important to consider the supply chain. Here, too, better monitoring enables prevention and detection.

"In the high tech industry, contract manufacturing is assumed. However our global supply operations evolved well beyond that," says John Haydon, vice president of global supply management for Nortel Networks Limited. "We've outsourced parts of the actual supply chain. In such complex outsourcing environments you have to work very closely with your outsourcing partners to minimize risks of counterfeiting."



Strong Response

A solid effort at prevention can diminish the need for detection and response. However, relying on prevention alone can cause you to lose sight of the bigger problem. Make sure the detection effort is strong (e.g., monitoring and auditing) but also be prepared to actively help law enforcement and other authorities. Some companies will even provide transportation for local authorities that plan to "raid" a suspected manufacturer or distributor. Others provide local law enforcement with tools it cannot afford to buy.

Establish Priorities and Build an Anticounterfeiting Organization

Unlike early warning signs, which can be detected without special organizational underpinnings, the above tactics require dedicated support. Therefore, prioritization is essential, as no company has unlimited resources for fighting counterfeiters. It's important to focus on the products that are most likely to be copied. Do the same for contract manufacturing and supply-chain vendors. Try to identify those who put you most at risk in terms of financial loss and damage to your brand. With regard to employees, be clear about work methods, but set solid boundaries with regard to activities that can increase counterfeiting. Be clear about the importance of adhering to security policies.

Basing People Locally

Counterfeiting mitigation is not a remote activity. You can only do so much from a centralized location. You need people to be present in key locations so they can carry out anticounterfeiting tactics.

Communicating Effectively

Communication plays a major role in counterfeiting mitigation. We have identified six separate stakeholder groups that should be in the communication loop.

Company Employees

Your internal people need to be aware of and properly trained to understand the problem and how they can help deal with it. This includes everyone from a repair technician who thinks a return may be counterfeit to a call center person explaining to a service customer that a product may be counterfeit.

Business Partners

Distributors, authorized resellers, and contract manufacturers need to be part of the solution. They need to understand the importance of ferreting out counterfeit products and being on the same team as you.

Independent Distributors

Some companies avoid communicating with independent distributors as a way of showing their disapproval of grey-market activities. This, however, can work against them because independent distributors are the likely channels for counterfeit products, many of them unwittingly. An open communications channel allows them to query OEMs about suspicious products and help keep counterfeit products out of circulation.

National and Local Governments

In some countries it's important to communicate with both national and local governments. Coordinated pressure on national governments may help pass legislation that offers intellectual property more protection. Individualized attention to local governments may help to enforce the laws where the need is greatest.

Your Customers

Customer communication is also important, but requires delicacy. You do not want to create an impression that your product is being heavily counterfeited; you do want customers to take responsibility for buying from authorized sources. Every company must decide for itself to what degree it will accommodate customers, but the key message in all cases needs to be "let the buyer beware" when purchasing from independent channels. Consumers should be encouraged to buy from authorized sources or directly from manufacturers to avoid counterfeits and to ensure products are fully warranted.

Industry Groups

As any security organization will attest, benchmarking, sharing best practices, and pooling information are important elements of an anticounterfeiting strategy. A first step is benchmarking against what other companies have done or are doing. Industry alliances such as AGMA can be great forums for benchmarking and sharing best-practice ideas, and for innovating new ideas.

Putting It All Together

No anticounterfeiting effort is entirely foolproof, but the better ones can make a significant difference. The products most likely to be counterfeited are those with broad brand appeal, high volume, and respectable margins. OEMs should make these products more difficult to copy. Just as pharmaceutical companies have trained us not to accept a bottle with a broken seal, high technology companies need to integrate authenticity identifiers into their products and train customers in what to look for.

Anticounterfeiting programs benefit most from high-level sponsorship within a company—ideally at the executive level. Executive leadership will drive receptivity and participation in education and training programs that can help mitigate the threat of counterfeiting.

Board members and audit committees should also ask for evidence that counterfeiting is not materially compromising a company's financial results. And, they should require the internal auditor to report on the company's anticounterfeiting measures. Whatever approach a company adopts, it should be tailored to the company's specific issues. Once identified, the needs should be prioritized and organized for swift and decisive action. The people chosen, as well as their tasks and activities, should adhere to clearly defined methods and policies. This group should be responsible for helping to detect, respond to, and prevent instances of counterfeiting, including encouraging the engineering function to design products that are harder to copy. It should have "feelers" into internal and external data sources that can help monitor and audit supply, manufacturing, and distribution. It should be empowered to collaborate with industry groups that specialize in helping companies fight counterfeiting.

When counterfeiting is detected, the company must be prepared to take a tough, prosecutorial stance.

The organization should also have people permanently located in countries deemed high risk. This will allow more effective detection and quicker response. And, when counterfeiting is detected, the company must be prepared to take a tough, prosecutorial stance. Ideally, every company's objective should be becoming the least attractive counterfeiting target in its industry.

KPMG's Electronics, Software & Services Practice

Our Electronics, Software & Services practice can help OEMs with the prevention of counterfeiting. This practice comprises multidisciplinary professionals from KPMG member firms who can assist clients in their efforts to achieve high levels of business integrity through the detection, prevention, and investigation of counterfeiting, fraud, and misconduct. We not only help clients discover the underlying facts but also assist in assessing vulnerabilities and in developing controls and programs to address risks.

Professionals in KPMG's Electronics, Software & Services practice draw on extensive experience in contract compliance, forensic accounting, law enforcement, fraud and misconduct risk assessment, antifraud risk controls, program design and implementation, asset tracing, computer forensics, and forensic data analysis.

For more information, please contact:

Gary Matuszak
Electronics, Software & Services
KPMG in the United States
+1 (650) 404-4858
gmatuszak@kpmg.com

Adam D. Bates
KPMG Forensic
KPMG in the United Kingdom
+44 (0) 20 7311 3934
adambates@kpmg.co.uk

Richard H. Girgenti
KPMG Forensic
KPMG in the United States
+1 (212) 872-6953
rgirgenti@kpmg.com

David J. Van Homrigh
KPMG Forensic
KPMG in Australia
+61 (7) 3233-3205
djvanhomrigh@kpmg.com.au

Petrus J. Marais
KPMG Forensic
KPMG in South Africa
+27 (21) 408-7022
pmarais@kpmg.co.za

Jim Hunter
KPMG Forensic
KPMG in Canada
+1 416 777 3193
jameshunter@kpmg.ca

Mark Bowra
KPMG Forensic
KPMG in China
+86 (21) 6288 3053
mark.bowra@kpmg.com.cn

About AGMA

The goals of the Alliance for Gray Market and Counterfeit Abatement are to protect the authorized distribution channels and intellectual property of authorized goods to improve customer satisfaction and preserve brand integrity.

The Alliance is a nonprofit organization composed of companies in the technology sector. AGMA's mission is to mitigate the gray marketing fraud and counterfeiting of technology products around the globe. AGMA is one of the IT industry's leading trade groups addressing counterfeit issues. The organization's charter includes development of best practices for mitigating the counterfeiting of branded technology products and the potential harm it causes to end customers, authorized or approved channel distribution partners, and the high tech industry as a whole.

Reducing counterfeiting and gray marketing activity is important for maintaining high standards of product quality and reliability—and for ensuring that customers' service and support requirements are met. By working in cooperation, member companies implement practical and effective deterrents to both the gray-marketing and counterfeiting of high tech products to protect intellectual property, trademarks, and copyrights as well as to preserve brand equity.

The financial impact and customer satisfaction issues are significant. The inherent value of a brand is strengthened when products are delivered through approved distribution partners, ensuring the highest quality product and the best possible service and support for customers. Also, by addressing unauthorized gray market activity, a level playing field is created for authorized distribution partners.

AGMA also established the Gray Market/Counterfeit Tip Line in efforts to help serve customers and preserve their user experience. If you believe that you are aware of counterfeiting activities or illegal gray market diversion, you can contact this confidential e-mail address: tipline@agmaglobal.org.

For more information from AGMA, please contact:

Marla Briscoe
Vice President
+1 (281) 518-7818
marla.briscoe@hp.com

Lily Mei
Executive Director
+1 (510) 252-9888
lily.mei@agmaglobal.org

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.