

Intellectual Property Fraud Protection




"GSA commissioned New Momentum to offer this paper."

Authors |

Chris Jensen is a Vice President at New Momentum (San Clemente, CA), a company that provides brand/IP Protection software to the electronics industry.

Raminderpal Singh is a Senior Technical Staff Member, of IBM's 300mm Semiconductor Fab, Systems and Technology Group's Transformation Core.

Do you know what counterfeits are costing your company?



Outsourcing and globalization have numerous benefits, but they have a significant downside—the proliferation of counterfeits and sales through unauthorized channels. Semiconductor manufacturers are losing billions every year to counterfeits and the gray market. In 2006 U.S. Customs recorded over 15 billion IC imports--about 500 every second. Results of a study conducted by AGMA (Association for Abatement of Gray Market and Counterfeits) and KPMG, showed that one out of every ten IT products contains counterfeit semiconductors. That means 1.5 billion of those imported ICs are likely counterfeit...about 50 counterfeits every second flooding into the US. Do you know how many of those 1.5 billion (and the number is growing all the time) are yours? Most semiconductor manufacturers don't realize the extent of their revenue loss to counterfeits.

And, revenues are not all you are losing. Company and product reputations are being eroded and legitimate channel partners lost. The goal of this paper is to demonstrate the impact counterfeits have on semiconductor companies as well as provide you with solutions to stop these unauthorized sales. And most importantly, this paper will show you why semiconductor companies need to take action now before your revenues and reputation are eroded even further. Participation in the GSA's IP Protection working group is an important step.

In 2006 U.S. Customs recorded over 15 billion IC imports--about 500 every second.

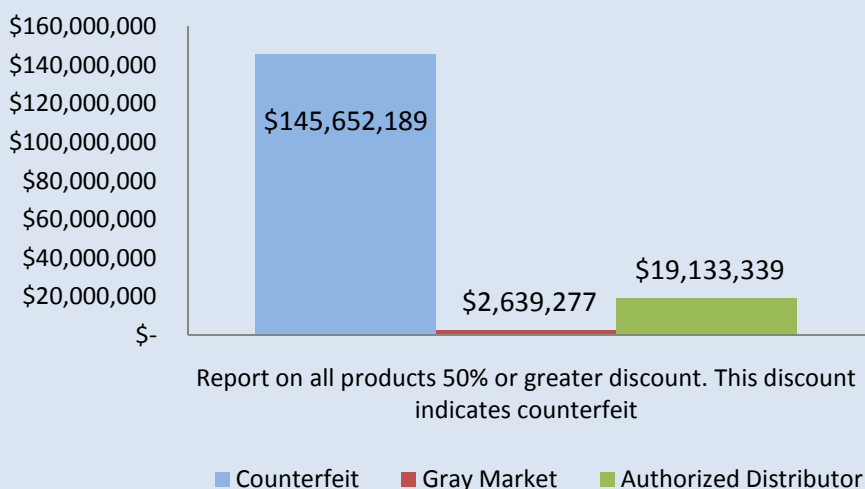
Why is now the time to take action?

Once thought to be too complex and sophisticated for counterfeiters, semiconductors, electronics and IT (information technology) products are now hot ticket items in counterfeit manufacturing. Lost sales, however, only account for a fraction of what companies sacrifice when their intellectual property (IP) is stolen and their products illegally produced.

Counterfeiters steal IP backed by million-dollar investments in research and development, marketing, and manufacturing. Moreover, illegitimate or substandard chips present the company with additional costs to repair or replace defective products carrying their brand name.

Potential Counterfeit Activity *by Revenue Loss*

Study | 1 Global Semiconductor Company from Jan 23 – Feb 18, 2008



The Semiconductor Industry Associate (SIA) recently formed an Anti-Counterfeiting Task Force that conducted a study with these results:

Company A: Over 100 part numbers have been counterfeited in the last 5 years

Company B: 19 cases reported with 97,000 units

Company C: Since June 2006 there have been 4 US Customs seizures of counterfeits of our products by US Customs; units seized ranged from 6,000 to 60,000

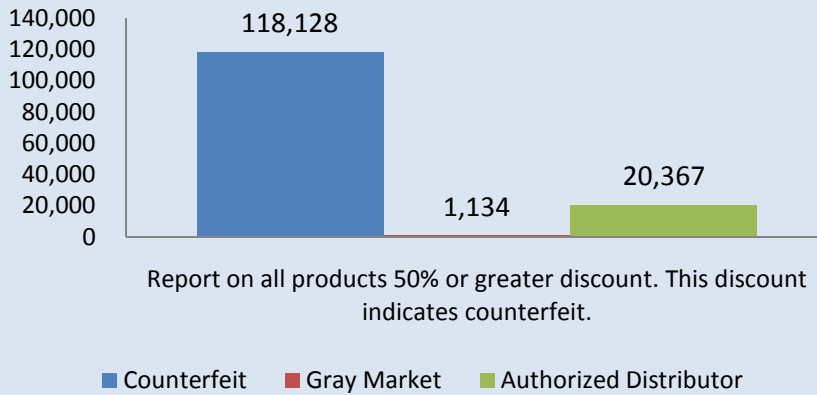
Company D: We estimate that 2-3% of the purchases of our brand are counterfeit

Company E: A broker website indicated 40,000 of our devices available, but our company had only made 200 units of that device with the specified date code. If all 40,000 were available, it would result in a \$34 million loss.

Can your company afford these kinds of losses? By the way, this is the activity these companies found without using the advanced technologies that would give them even greater visibility into counterfeit activity.

Potential Counterfeit Activity by Quantity

Study | 1 Global Semiconductor Company from Jan 23 – Feb 18, 2008



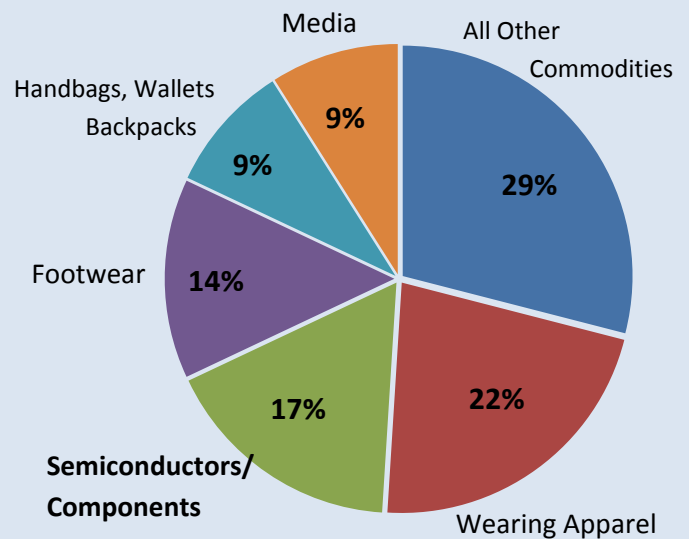
A number of factors have coalesced to create a business environment in which manufacturing counterfeit IP is not only lucrative, but also much more attainable than ever before. Counterfeiters are becoming increasingly tech savvy, and their ability to obtain more advanced manufacturing machinery and techniques has been one of the most crucial factors in fueling the production of illegal high-tech goods.

During the past decade, billions of dollars in foreign direct investment (FDI) have flowed into a number of developing countries, such as China, leading to the proliferation of sophisticated manufacturing processes and capabilities to produce high-tech products. Counterfeit components have long been a problem in the electronics industry, but as of late, companies are finding themselves increasingly challenged with having to deal with counterfeit semiconductor components.

A second contributing factor is the popularity of e-commerce. Many counterfeiters are using the Internet to reach potential buyers, and without regulatory bodies able to police and govern all product-listing sites or advertisements sent out over email, the Web has become a bastion for illegal sales of counterfeit products.

Top Products Seized

Source | U.S. Customs and Border Protection



Why is the problem becoming more serious for semiconductor companies?

Remarking one of the biggest problems

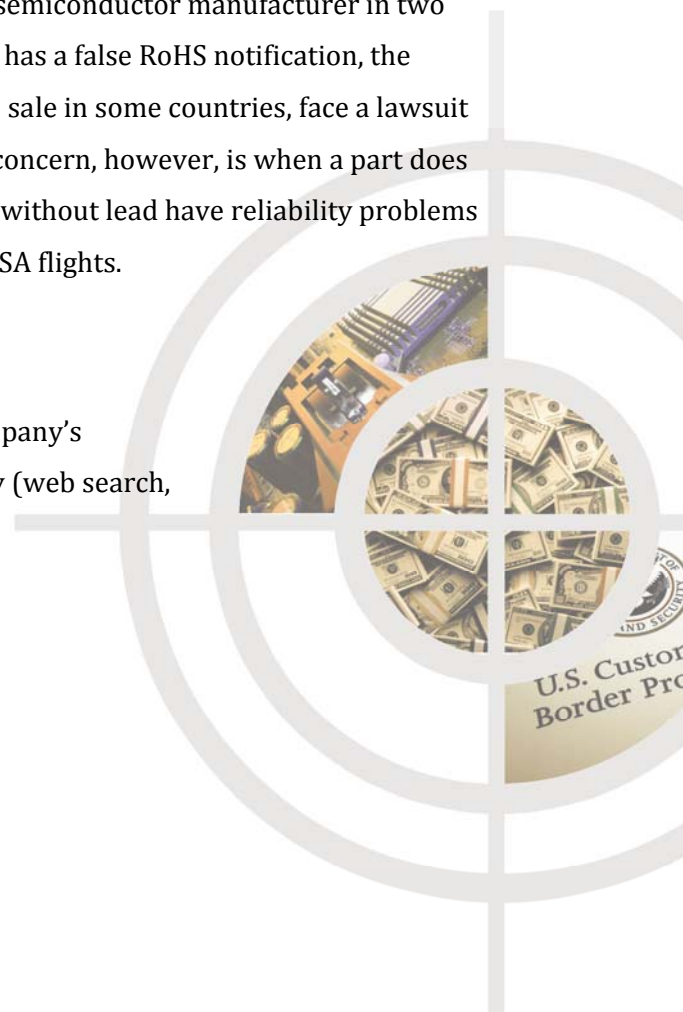
In the SIA study, remarking was the most common method of counterfeiting. Remarking involves scraping a label off a chip package and printing on a new label. This can involve a different and higher-priced brand, or a faster chip speed, or a military grade lot number on a commercial chip. Most of the problem is coming from Shenzhen China, located on the border with Hong Kong. You can find anything in Shenzhen—original, fake, new, and old components. It's common to find shops making fake "Samsung, Motorola," etc. labels. The Chinese vendors say that making the labels is easy—they simply select the specific component maker's label from the program library, then modify the data. The label quality is excellent.

Other counterfeiting tricks include incorrect die, inferior packaging materials, reproduction of chip designs, packages without die, different labels on packages, false RoHS (Restriction on Hazardous Substances) notifications.

Inaccurate notifications of whether a chip has lead can impact a semiconductor manufacturer in two different, yet significant ways. First, if the chip contains lead but has a false RoHS notification, the semiconductor manufacturer may have products restricted from sale in some countries, face a lawsuit and experience significant amounts of bad publicity. Of greater concern, however, is when a part does not contain lead and the counterfeiter asserts that it does. Parts without lead have reliability problems when used in applications in outer space such as satellites or NASA flights.

How can you solve this problem?

There are several key areas you can focus on to reduce your company's revenue erosion from counterfeits: legal, operational, technology (web search, encryption, lock & key).



What can you do through the legal system?

Though many big players in the IT industry are making headlines as they break up crime rings, small-to-midsize enterprises face a tough fight in their struggle to protect their IP; a number of internal and external issues challenge companies' ability to find, identify, and persecute transgressors.

How about encouraging US Customs to make semiconductor counterfeiting a priority? While it may be easier to spot counterfeit luxury goods, fake semiconductors can result much more dangerous (even deadly in the case of medical devices) situations.

How about the operational approach?

One important step in reducing counterfeiting is to focus on illegal sales on the gray market. While some gray market brokers are legitimate, the gray market is an excellent outlet for counterfeits. AGMA says, suggests examining companies trying to enter distribution channels and monitoring contract manufacturers and distributors already in the supply chain. The organization recommends thoroughly interviewing companies and investigating their background before allowing them to become resellers or distributors. Once they enter the supply chain, AGMA advises organizations to establish strict contracts, perform extensive auditing, and maintain close relationships with its outsourcing partnerships.

Though the listings may be hidden in the deep recesses of the Internet, a couple effective search words can bring up product listing after product listing of both legitimate and counterfeit goods.

Technology-web search

Many companies that have resorted to manually scouring the Web for unauthorized product listings and counterfeit goods have found this process time consuming, tedious and ineffective.

The up-and-coming technology is based on the collection and organization of unstructured data. Unstructured data is information collected from a number of electronic sources that hasn't been arranged or organized into an understandable form. In the context of seeking out product listings, this data can come from a number of sources including market Web sources, XML data sources, B2B sites, forums, auctions, and emails advertising gray market sales.

Results of a study conducted by AGMA (Association for Abatement of Gray Market and Counterfeits) and KPMG, showed that one out of every ten IT products contains counterfeit semiconductors.

Software solutions like this bring a number of benefits to manufacturers. Not only does it eliminate the significant number of man hours and resources manual searching required, these systems can tap into information sources previously out of reach by traditional search methods and thereby increasing the amount of “area” a company can keep a watch on the marketplace.

They also highlight other market activity exceptions, such as new sellers entering the market and an unexpected amount of selling or buying in a particular geographical region.

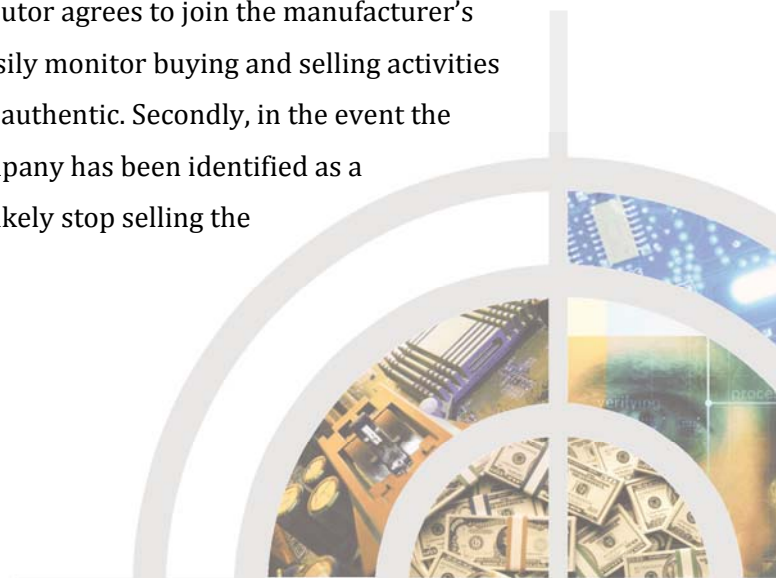
When looking for an IP-protection solution, make sure all reports and data collected are accessible through a Web portal and that the supplier is a Software as a Service (SaaS) supplier. This makes data immediately available without any extensive installation processes and, more importantly, without the involvement of other departments that may slow the deployment down.

Case Study

One Tier 1 fabless semiconductor manufacturer has already deployed this kind of system and saw an immediate return on investment. In the first 30 days, the manufacturer found 500 cases of unauthorized sales or counterfeit products previously undetected by its traditional monitoring systems. Over a year’s time, if 6,000 unapproved transactions were prevented, the manufacturer could save itself millions of dollars in lost revenue.

Collecting data and reports, however, doesn’t necessarily result in a decrease in counterfeiting; the information needs to be put into action. Often times when companies manage to receive timely data on counterfeits or illegal gray market sales, they simply don’t know what to do with it. The above manufacturer handled one of its instances of unauthorized sales through an unconventional route: it tried to turn unauthorized distributors into legitimate ones.

The benefit of this strategy is two-fold. First, if the distributor agrees to join the manufacturer’s authorized channels, the manufacturer can then more easily monitor buying and selling activities and more effectively ensure the products distributed are authentic. Secondly, in the event the distributor declines the offer, its managers know the company has been identified as a counterfeiter or an unauthorized sales channel and will likely stop selling the manufacturer’s product.



The call to action

Another significant obstacle to successfully addressing counterfeiting problems has been underestimating the problem due to the lack of dialogue and understanding of the enormity of the problem in the semiconductor industry. Typically, companies grappling with counterfeiting shy away from publicizing the problem, and this relative silence have led many in the industry to underestimate the enormity of counterfeiting and the amount of assets at stake. It's time to take a stand against counterfeiting, and push forward toward effective solutions to this problem.

Here's how you can participate:

Attend GSA's webinar focusing on IP Fraud Protection.

October 8, 2008 at 10 am Pacific time

No semiconductor company, no matter how large or small, is immune to IP fraud problems. Speakers will discuss how counterfeits are impacting the semiconductor industry, how to determine what it may be costing your company and how you can combat the problem.

To register for the **free** webinar or for more information, visit:

<http://www.gsaglobal.org/publications/ipfraud>

Or contact:

GSA: Lisa Tafoya, ltafoya@gsaglobal.org

New Momentum: Chris Jensen, cjensen@newmo.com