

Fighting High-Tech Counterfeiting

with High-Tech Solutions

Facing the possibility of losing more than \$100 billion in revenue each year, global IT companies need a multi-front offense to combat counterfeiting and supply-chain risk management software solutions promises to be a key factor in that strategy.

NEW MOMENTUM

New Momentum offers brand protection solutions for manufacturers who make or use electronic components. With a focus on supply chain risk management, New Momentum's software solution allows manufacturers to constantly monitor the open marketplace through the collection of global buying and selling transaction data from Web sources. The San Clemente, Calif.-based company also provides services for supply interruption, partner compliance, and asset valuation applications.

www.newmo.com

Each year the U.S. Customs and Border Patrol confiscates millions of dollars in counterfeit goods. In 2006 alone, products seized by U.S. officials totaled more than \$155 million. Unfortunately, even as the agency sees significant growth in the amount of counterfeit products detained from year to year—2006 marked an 83% increase from 2005—efforts to sniff out unauthentic goods through customs and border patrols are only capturing a small fraction of a multi-billion dollar problem.

The U.S. Chamber of Commerce estimates American companies lose \$250 billion in sales every year as a direct result of counterfeiting and piracy. Even in the face of rising awareness among consumers and collaborative efforts among government organizations, the Chamber says the problem is continuing to grow at an alarming rate.

Fake high-end designer clothing was at one time the symbol for the world's counterfeiting problems. Today, 22% of all clothing and footwear sold worldwide is counterfeit, according to industry estimates. Despite these alarming estimates, the tides are turning and the problem is reaching far beyond the apparel industry and into every aspect of the American economy. In total, the business lost to counterfeiting is estimated to represent as much as 6% of world trade, according to International Chamber of Commerce.

Once thought to be too complex and sophisticated for counterfeiters, electronics and IT (information technology) products are becoming the next hot ticket item in counterfeit manufacturing. The Alliance for Gray Market and Counterfeit Abatement (AGMA) estimates one out of every 10 IT products are counterfeit or contain partial counterfeit parts.

U.S. Customs and Border officials are also seeing a steep increase in the amount of illegally produced IT goods. At the midpoint of fiscal year 2006, the agency had confiscated approximately \$8 million in computers and hardware, a 1,142% increase as compared to the same time period in 2005. Officials say notebook computers accounted for almost 50% of the total while networking hardware comprised another 25%.

Lost sales, however, only account for a fraction of what companies sacrifice when their intellectual property is stolen and their products illegally produced. Counterfeiters steal intellectual property backed by million-dollar investments in research and development, marketing, and manufacturing. Moreover, illegitimate or substandard goods can not only severely damage a brand's marketplace equity, but also present the company with additional costs to repair or replace defective products carrying their brand name.

83%

U.S. Customs and Border Patrol has seen an 83% jump in the amount of confiscated counterfeit goods between 2005 and 2006.

A number of factors have coalesced to create a business environment in which manufacturing counterfeit IT goods 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 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 challenged with having to deal with counterfeit semiconductor components as well.

Secondly, IT products yield a much higher profit per unit than many other products. Whereas imitation purses or wallets can be sold for \$20 a piece on street corners, consumers may willingly spend thousands of dollars on counterfeit laptop computers.

A third 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.

Underestimating the Problem

Billions of dollars are at stake in the battle to protect IP. In a July 2007 raid, American and Chinese authorities seized more than \$7 million in assets, including more than 290,000 counterfeit software CDs and certificate of authenticity in what was a two-year-old operation. The software was estimated to have a street value of about \$500 million. Redmond, Wash.-based Microsoft Corp. estimates that the

piracy of these counterfeit operations has cost the software giant at least \$2 billion in lost revenue during the past six years.

Electronic component manufacturers are seeing similar losses in revenue. At its annual partner conference in April 2007, San Jose, Calif.-based Cisco Systems said sales of its goods in unauthorized channels cut switch and router revenues by 7% in one year alone. Cisco's switches and routers represent a \$3.5 billion business unit, and for an electronics manufacturer of similar size, even a 5% drop in revenue due to counterfeiting could mean a \$179 million loss.

Cisco's total losses, however, don't simply end with year-end revenue. According to the manufacturer, much of the unauthorized sales occurred within the SMB (small-to-midsize business) market, an area in which Cisco is trying to expand. Thus, heavily discounted prices and damage to brand reputation possibly incurred by unauthorized vendors and counterfeiters selling to the SMB market presents Cisco with the likelihood of losing many more millions of dollars in future sales and revenues.

Though many big players in the IT industry, such as Microsoft, 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.

One of the biggest obstacles is inconsistent enforcement of IP-protection laws from country to country. Ineffective law enforcement, which tends to be characteristic of developing and third world countries, is a significant catalyst for fostering hot spots for counterfeiting.

Since the centers of many counterfeiting operations lie outside the reach of U.S. law and governance, attempts to impose American laws and penalties associated with IP theft are often fruitless or at the very least frustrating and resource consuming.

In a 2007 report submitted to the Office of United States Trade Representative, the International Anticounterfeiting Coalition (IACC) reiterated its previous recommendations that U.S. agencies continue their anticounterfeiting efforts in China.

In recent years, China has embarked on a number of collaborative efforts with U.S. officials to weed out counterfeiting operations. In 2004, the U.S. Chamber of Commerce began working with the national Chinese government to reform its laws regulating IP use. More over, governments at the province level are also partnering with the Chamber to ensure compliance with new IP laws and to establish a method of measuring enforcement progress.

These initiatives are still relatively young, and like other nations placed on the IACC's "watch list," such as Brazil, Vietnam, Malaysia, and Mexico, efforts to stop

1,142%

U.S. Customs and Border Patrol says the value of seized counterfeit computers and hardware is up 1,142%.

counterfeiting operations in China have been hindered by the lack of coordination between national and local agencies and the sheer number and embeddedness of these illegal businesses. Add in the geographical shift of counterfeiting operations from Asia to regions like Eastern Europe, and it creates a climate in which manufacturers struggle to keep pace with a rapidly growing problem.

Many electronics manufacturers admit using traditional, judicial channels are no longer effective when it comes to finding and prosecuting counterfeiting and IP thieves. One such company, Orlando, Fla.-based Super Vision Intl., a manufacturer of LED lighting products for electronic displays, now known as Nexxus Lighting, saw first hand how limited government assistance could be. In September of 2002, Super Vision was awarded \$33.1 million in damages after a host of Shanghai and Hong Kong competitors were found guilty of stealing the company's trade secrets. The settlement should have been the largest trade-secret theft verdict in Florida's history, but instead it became an endless battle to collect the damages and shut down the counterfeiting operations, with uncooperative national governments and bureaucratic red tape within the American judicial system as the biggest hindrances.

Super Vision Founder Brett Kingstone says when it comes to IP there are more effective resources than the government. He adds that the only way to end counterfeiting is to punish those who steal IP and illegally produce goods, and until the U.S. government can step in and enforce intellectual property rights overseas, there is very little to accomplish through the civil process. Kingstone insists that manufacturers must do more for themselves if they want to ensure the protection of their products now and into the future. At the end of the day, he says, chasing counterfeiters through the judicial systems can require an "unlimited amount of years and unlimited amount of money," but taking on IP protection through unconventional means, such as keeping a close eye on international distributors in the supply chain, may be a one of the only effective ways for companies to make the most of its resources.

The gray market, an unauthorized distribution channel through which new, authentic products are sold without the permission or knowledge of the OEM (original-equipment manufacturer), also poses a great risk to a company's IP.

Industry observers are quick to reaffirm that counterfeiting often follows gray marketing. Marie Myers, former president of AGMA, was quoted in an AGMA and KPMG LLP joint document saying, "Counterfeiting and gray market channels often go hand-in-hand." Peter Hlavnicka, treasurer and board member for AGMA, adds that counterfeiting within the gray market extends well beyond simply product sales. He says, "The impact of counterfeiting is always greater than the value of actual counterfeit goods because it is detrimental to the brand owner...There's impact on the brand image, customer loyalty, and overall customer satisfaction." Despite the common negative dialogue that saturates debates on the gray market, few in the industry will outwardly admit the necessity of gray channels. Many

\$2 Billion

Microsoft estimated that as a result of one Chinese counterfeiting operation it lost \$2 billion in lost revenue over six years.

legitimate components and finished goods that end up on the gray market were once surplus stock “dumped” by third-party manufacturers and distributors without the OEM’s knowledge. In rapidly growing industries like information technology, products and parts are in constant demand, and often times one of the only efficient ways for legitimate companies to overcome shortages is to purchase needed parts from the gray market.

Brokers and distributors operating in the gray market channels aren’t necessarily illegally selling products. In fact, many of the transactions that go through these channels are legitimate, but movement of goods from one dealer to another makes it extremely difficult to determine the source and authenticity of the product. In the end, the very nature of the gray market makes it a necessary sales channel, but also a significant threat to the businesses it serves.

Another significant obstacle to successfully addressing counterfeiting problems has been the lack of dialogue—both vertically and horizontally—on the issue at hand. Typically, companies grappling with counterfeiting shy away from publicizing the problem, and this relative silence has led many in the industry to underestimate the enormity of counterfeiting and the amount of assets at stake. For example, semiconductor industry research indicates that there is \$40 billion in revenues in gray market activity.

Moreover, this lack of dialogue from companies dealing with counterfeits or sales through unauthorized channels is masking the magnitude of the issues’ impact on a company’s bottom line and could be a factor in a major internal challenge—businesses’ low prioritization of counterfeiting issues. According to a study conducted by consulting firm PricewaterhouseCoopers, the vast majority of respondents believed their organizations needed to increase the importance of IP. However, PricewaterhouseCoopers found only 21% of companies have departments dedicated to IP management despite the high price they are paying in revenue erosion.

Results of the survey also hinted that IP’s low position on the priority totem pole could be a result of executive’s reliance on laws and judicial systems to keep their intellectual property safe. Research showed that 69% of executives, the majority of whom represented North American or Asian businesses, reported that IP issues were too often handed off to the legal department and treated as a legal issue.

But the reality of the industry’s counterfeiting problem is that the issue has grown well beyond the reach of judicial bodies. It’s now a sales problem, a revenue problem, a distribution channel problem, and the numbers prove it. Cisco estimated competing unauthentic goods in gray market distribution channels cost the company between \$200 and \$300 million in lost revenue during FY 2006.

Whereas legal departments may have a role in mitigating counterfeiting, the widely apparent effects of IP theft on year-end and future revenues demonstrates

**\$200-\$300
million**

Cisco estimated competing gray market sales cost the company between \$200 and \$300 million in lost revenue during FY 2006.

that it's time for companies to move beyond dependence on judicial systems and attack the problem themselves head on.

The Multi-Front Offense

Catching transgressors can be a tricky business, but it's not an impossible task. There's no silver bullet to the international counterfeiting problem; rather, companies need to build a multi-front offense.

In March 2006, the White House announced an initiative to crack down on IP theft. The Strategy Targeting Organized Piracy program, brought together nine federal agencies, including the Dept. of Justice, the U.S. Attorneys' office, and the FBI, to improve anticounterfeiting efforts in the U.S. Non-profit and trade organizations, such as the IACC and AGMA, a trade organization of high-tech companies, are also leading many partnership-building initiatives among industry members.

On an industry level, communication among companies is crucial to enabling the industry as a whole to effectively combat counterfeiting. Industry leaders are beginning to develop a dialogue, and recently publicized seizures and a number of health and safety concerns have brought to light some much-needed discussion of the problem.

One of these catalysts relates back to an initiative to phase in RoHS (Restriction of the Use of Certain Hazardous Substances) and WEEE (Waste Electrical and Electronic Equipment)-compliant parts. Spawning from a 2005 EU directive to make product components lead free (RoHS) and the disposal of waste from manufacturing processes more environmentally friendly (WEEE), all companies selling products in Europe or providing components to European manufacturers recently began to spec new parts.

As companies spec any new component, they increase their risk of coming across fake parts. The reason is simple: changes to components—in this case replacing lead-containing parts with lead-free ones—require adjustments to manufacturers' bill of materials. And when components are being switched out for others en masse, the risk of sub-standard parts finding their way into supplies of legitimate products rises.

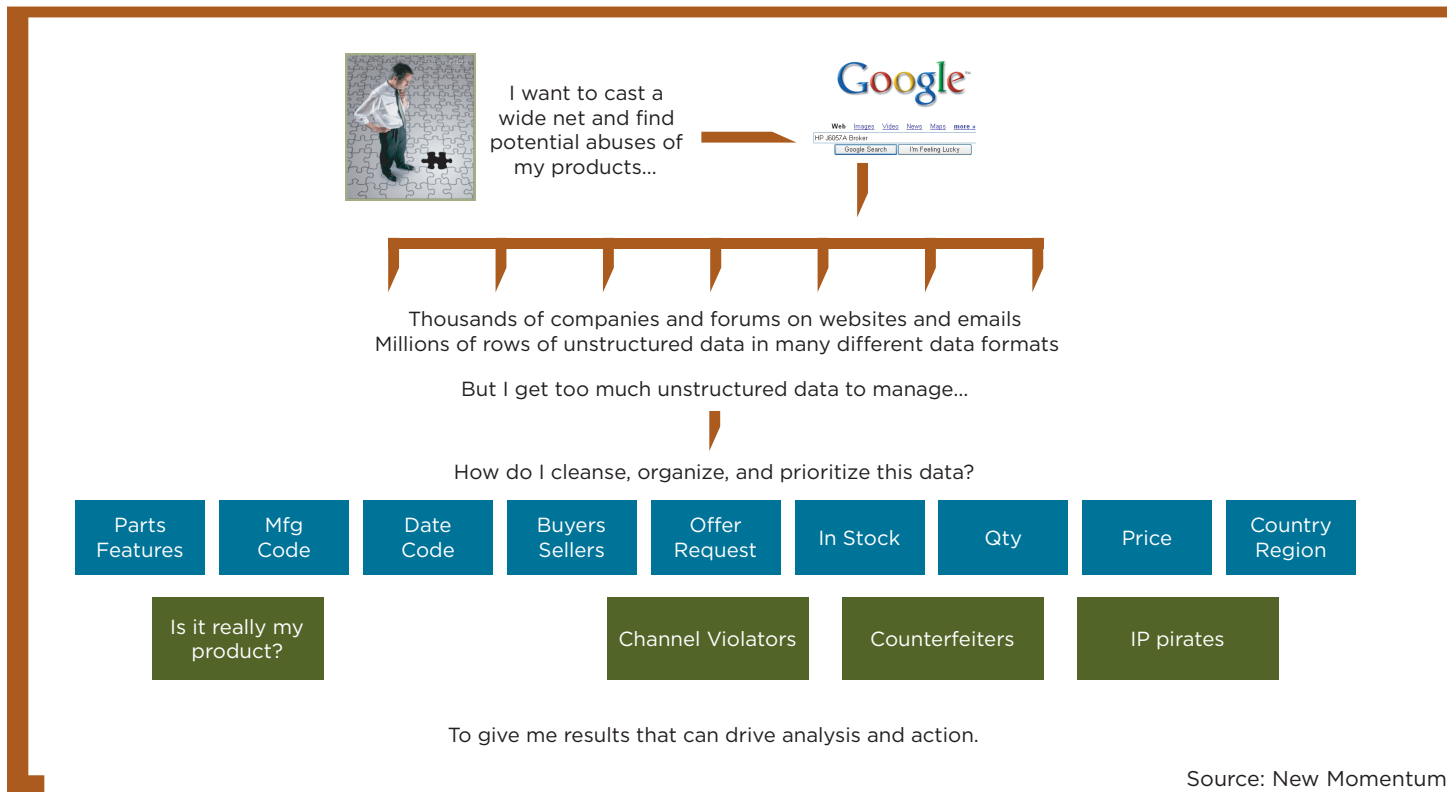
In addition to encouraging discussion on counterfeiting issues within and across industries, the problem also needs to be tackled on an operational level. One important step in reducing counterfeiting and illegal sales on the gray market, AGMA says, is carefully examining companies trying to enter distribution channels and monitoring contract manufacturers and distributors already in the supply chain. The organization suggests 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.

What many companies have resorted to doing is manually scouring the Web for unauthorized product listings and counterfeit goods. With more and more counterfeiters and unauthorized sales taking their operations to the Web, everyday search engines like Google often times pick up listings of counterfeit product on the market. 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.

The traditional way of monitoring the Internet to protect IP consists of a tedious and resource-consuming process of Web crawling. The search begins with determining the correct search terms—products names, part numbers, etc.—that will yield the most amount of hits for a company’s products. The terms are then used in a Google search to pull product data from available Websites and emails. The most common search engines, such as Google and Yahoo, can reach thousands of company’s Websites and sales forums, presenting organizations with the opportunity to remotely search a wide range of sales channels using in-house PCs. Yet, the immense number of available data sources also results in an unmanageable amount of collected information. A Google search for a single component can draw millions of rows of unorganized data in a number of different formats.

After collecting the data, it must then be sorted through to eliminate any duplicated information and to ensure the component listings retrieved do represent the illegally produced and distributed components the company set out to find. This requires cross checking part features, manufacturing codes, data codes, offer requests, and a number of other characteristics against the aggregated data and

BP SEARCH



the company's product specs and lists of authorized sales partners and distributors. Once the raw data is "cleansed," it still requires further time-consuming organization and analysis to become actionable data for decisionmakers.

The sheer amount of information makes it extremely cost prohibitive to perform these searches on a regular or consistent basis. Because cracking down on unauthorized sales on the gray market requires vigilance, the significant time lag between data collection and data analysis and the inevitable lapse in monitoring that characterize manual Web searches creates holes in companies' IP defense.

For example, if an electronic component manufacturer attempts a manually scour the Web, new listings could appear and disappear in the long interim between searches. Moreover, market conditions could change during the time it takes for raw data to turn into actionable data, and crucial decision related to IP protection strategies could be outdated, and more importantly ineffective, by the time they're implemented. This could mean millions of dollars of lost revenue each year that the manufacturer isn't even aware of and isn't able to stop.

The ineffectiveness of manual wide-net casts, however, is no indication of the Internet's true potential in helping companies catch counterfeiters. The Web is likely one of most valuable resources a company has; the data simply needs to be captured and organized in a more effective, more efficient way. Automating the search and analysis process in one way to dramatically reduce the overhead costs associated with wide net search, and a few technology providers are stepping up to the plate to provide manufacturers with the technology solution to do just that.

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, and emails advertising gray market sales.

Counterfeiting by the Numbers

\$600 Billion:	Estimated annual sales of counterfeit products worldwide.
\$23 Billion:	Estimated yearly sales of counterfeit products in New York City.
\$20 Billion:	Minimum estimated loss American companies suffer due to counterfeit products.
\$1 Billion:	Minimum estimated loss in tax revenues in New York City due to counterfeiting.
\$155 Million:	Estimated domestic value of counterfeit goods confiscated by U.S. Customs in 2006.
7:	Percentage of world trade represented by counterfeit goods.

Source: International Anticounterfeiting Coalition (IACC)

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.

Very few software developers are dipping their feet into the unstructured data pool, and it may take some time

for the technology to enter the mainstream consciousness in manufacturing. Yet, New Momentum, a San Clemente, Calif.-based company that focuses on IP protection, has emerged as the first to successfully introduce these solutions to the marketplace.

Keeping an Eye on the Supply Chain

Over the past two years, New Momentum has acquired hundreds of millions of transactions, representing a true composite of global information, as well as parametric information on more than 90 million components manufactured over the past 30 years. For an electronics component manufacturer, the first step of New Momentum's process is setting up the correct search parameters to interrogate its vast historical, realtime database of gray market activity.

Depending on the solution, a number of different "groups" of search criteria is determined to yield the most thorough search possible, and these groups are set up as automatic watch lists with auto-feedback or by exception feedback to the user. Those groups can include software, or SDKs that allow the seller to program each chip type for use on a network; the current chip; the newest chipsets; as well as older chips.

Each major criteria group search consists of several subsearches where each item is searched for under its product family part number, its "street" part number, and any other ways the same product is named for different markets. Some software solutions also have the capability of searching for product features or capabilities as a way of identifying products.

Once all the raw data is collected, the next step is to begin organizing the information and confirming the product listings identified as the manufacturer's product are indeed the manufacturer's products. Misnamed products, duplicate entries, and any other incorrect or unusable are removed, leaving only "clean" data.

Then, the market data is integrated with the end user's structured enterprise data. After incorporating the company's production information, private client data, and customer risk models and pinpointing authorized partners, the software modifies its searches and expands its search to open-market selling and buying sites, forums, and individual companies. This expansive search results in the aggregation of both buying and selling solicitations along with what components were requested and detailed information on both the sellers and purchasers.

These wide net searchers can help manufacturers more effectively monitor the channels through which their products are sold. Depending on the end users' needs, collected data can be automatically organized and presented in detailed summary reports at set time intervals. Reports can range from trending charts according to product family; sales by geographical region, quantity, and number of buy/sell offers; and rankings of individual companies who buy and/or sell the largest quantities of the manufacturers' goods.

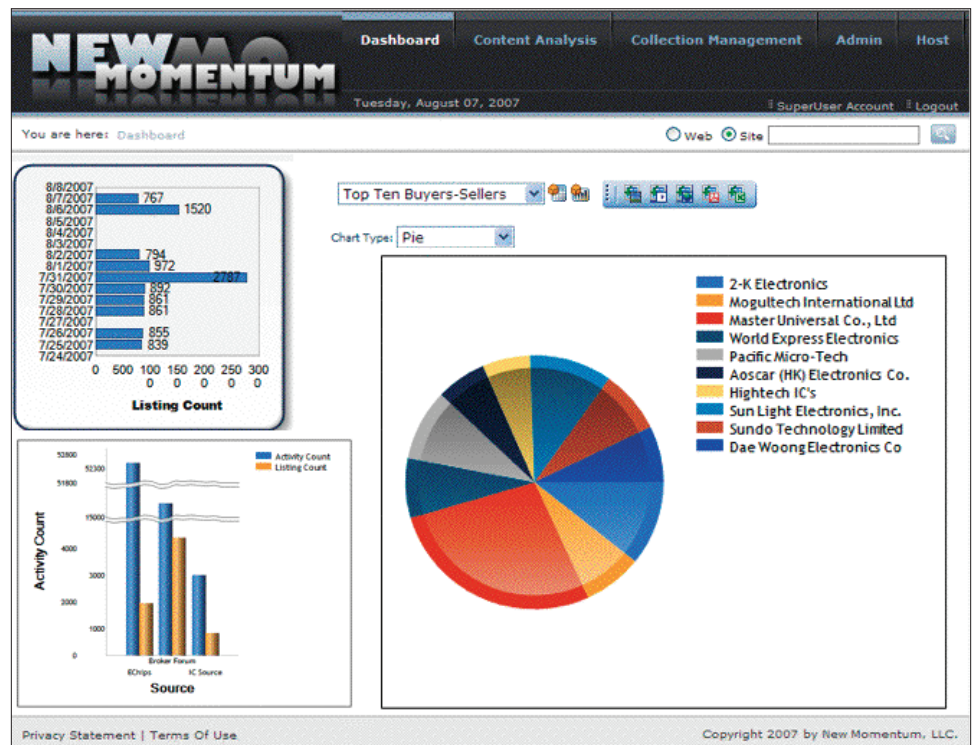
A number of aspects can trigger alerts. Customer can set tolerance levels, or threshold minimums and maximums, for a variety of indicators including percentage increase in market demand and percentage increase in offer quantities. The system also highlights other market activity exceptions such as new sellers entering the market and an unexpected amount of selling or buying in a particular geographical region.

One Tier 1 electronics manufacturer has already deployed the 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. New Momentum has honored its client's requests for total anonymity due to the highly sensitive nature of the brand/intellectual property protection business.

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 a legitimate ones.

BP Screenshot

Customers can easily view data collected by New Momentum's Brand Protection software with user-friendly dashboards. Data appears in graphs illustrating unauthorized sales trends according to product family, geographical region, number of buy/sell offers, individual companies, and a number of other categories.



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.

But in order to reach this strategy execution stage, companies have to implement the solution into their daily operations, a process that is much easier than most think. For example, New Momentum's solution jumps over a common hurdle for supply chain technology deployments: the IT department. In most high-tech manufacturing companies, protecting IP through supply chain risk management isn't an IT priority yet. Rather, the vast majority of companies' IT resources are dedicated to meeting mandates relating to internal security, firewalls, and preventing internal personnel from stealing documents or emailing them to unapproved sources. Moreover, many IT departments are often overwhelmed with work and trying to get managers to add another project to their lists and another expense to their budgets can be difficult.

All reports and data collected by New Momentum are accessible through a Web portal. Therefore, the customer can begin using the data immediately without any extensive installation processes and, more importantly, without the involvement of other departments that may slow the deployment down. In addition, the monitoring service eliminates the need to hire a research or clerk to do traditional searches, allowing brand protection or IP protection managers to take the service costs out of their budgets as opposed to searching for funds elsewhere. New Momentum uses the latest security technology for protecting a company's data.

New Momentum is addressing the problem of supply-chain risk management, including brand/intellectual property protection, with a new model for emerging software as a service (SaaS) application optimization. Software applications, content, and business rules and practices are integrated and can be set up uniquely for each application. In fact, New Momentum's approach of providing rapid ROI through a balanced solution of software content in business rules represents the way of the future for new software solutions in many markets. Importantly, New Momentum's patent-pending technology, while currently being applied to electronic components, is a general purpose technology that can be applied to other industries, including pharmaceuticals, retail, A&D, automotive, medical, and industrial manufacturing.

The fight to eliminate counterfeiting and product sales through unauthorized channels will likely be an uphill battle for some time. Until the American government can harmonize its intellectual property rights laws with those in other countries, manufacturers' only true option to ensure the integrity of its business is to take IP protection into their own hands.

