The Real Solution to Fake Parts

October 1, 2009

The high tech supply chain is more vulnerable to counterfeit components than ever before. With increasingly sophisticated criminals, the only way to protect the supply chain is through tools, technology, and new thinking about industrial aftermarkets.

Securing Supply Chains through Data Transparency and Better Market Design

The rise of counterfeiting in recent years has been astounding. The US economy loses some $250 billion annually with some three-quarters of a million jobs lost every year to what the Wall Street Journal has labeled as “nothing short of an economic crisis.” The pain reaches in to all corners of the economy, and the high technology manufacturing is no exception. Counterfeit electronic components can be found in all corners of high tech chain, from basic light switches and games to advanced medical scanners and telecommunications infrastructure. As electronic components find their way into more and more parts of modern life, the risk of counterfeit will threaten economic growth and consumer safety the world over. For the industry to successfully protect against this risk, we must understand its causes and how finds its way into the legitimate supply chain.

Size and Scope of the Problem

As with any illicit activity, it is notoriously difficult to get firm numbers on just how large the impact of counterfeit electronic components has been. Preliminary results from the US Department of Commerce’s study on the topic put the figure at $10 billion in 2008 for the US, just for fake semiconductors alone. A 2008 UK report calculated that the British economy suffers losses of some $2 billion annually. The pain is not just financial - intellectual property, jobs, manufacturing rework costs, warranties and returns, national security, and the end users’ health and safety are all at risk when counterfeit components infect the supply chain.

The UK’s Association of Franchised Distributors of Electronic Components published some startling figures at the cost of letting counterfeits penetrate the manufacturing process. The AFDEC figures put the cost of discovering and replacing a single component in the receiving process near US$0.40 at the time of the study in 2007. The cost spiked to nearly $40 when the fraud was not discovered until the component was on a warehouse shelf. Factoring in rework and replacement, the study placed the cost of replacing a counterfeit component once it had been mounted on a circuit board at over $400. Once the infected product shipped, with both warranty and recall costs incurred, the cost of

replacing a single counterfeit electronic component in the customer's ran to nearly $2500.

Counterfeiters have become very sophisticated in recent years, and their products penetrate the supply chain more deeply. Less frequently do inspections intercept fakes at the receiving dock. More and more, counterfeit parts pass initial testing make it into the end product. Manufactured without quality in mind, these illicit parts lack the durability of their authentic counterparts and will eventually fail in the field, at much greater cost to the manufacturer than if they had been detected at receiving.

These costs would be merely annoying if the incidence of counterfeit components had remained at historical levels. Since 2001, however, the frequency with which counterfeit parts have been found has increased many times over. Whereas fake components might once have represented a mere percentage point or two of all components sold in the secondary market, they now represent a much more significant fraction of that large market. IPC, the Association Connecting Manufacturers, released the findings of a study in 2008 which estimated that a stunning 13% of components sold in the secondary market were counterfeit. An October, 2008 article in *BusinessWeek* cited a US Defense Department estimate that counterfeit parts represented over 15% of components DOD contractors purchased from the secondary market.

It has been said that the only certain things in life are death, taxes, and inaccurate forecasts. Every firm, no matter how large or lean, will face regular shortages as part of their normal operations. As electronics become central to products across industries, more and more sectors of the economy will face the very real risk of counterfeit components. Counterfeit parts enter the supply chain via the secondary market, and since there is no plausible way to avoid shortages, executives across all sectors of industry must tackle this grave and growing problem head on.

Causes of Counterfeit

Several trends have created this crisis. Some are deep themes of the globalizing economy, others are very specific to the how transactions occur in the electronic components secondary market. None of them are likely to change anytime soon. Apart from a brief mention below, this paper will not examine the macro economic issues involved but will instead concentrate on the more immediate factors which drive illicit parts into the legitimate supply chain.

General

China

Over the last 10 years, the growth of manufacturing in China has been staggering. With annual growth rates in excess of 10% (and possibly much more, according to some analysts), the Chinese economy has grown so ferociously in the last decade, it is deeply enmeshed in almost every global supply chain. This move to becoming the "factory to the world" has included the wholesale relocation of manufacturing from high cost regions to China southeastern coast. As they have shifted manufacturing know-how and methods to China, western manufacturers have learned a painful lesson about the notoriously weak protections for intellectual property in China. Whereas a decade ago the counterfeiters used crude and shoddy techniques to create fakes, today they have access to the most modern tools and techniques and, in some cases, the original assembly lines themselves.

Lean

One of the most remarkable transformations of global manufacturing in the last few decades has been the proliferation of lean manufacturing. One of the core tenets of lean is the elimination of waste, to include unused inventory sitting in warehouses in the form of buffer stocks. As supply chains have become more efficient, many firms have struggled to implement lean methodologies properly across their supply base, leaving themselves with practically no inventory in times of heightened demand. Suppliers have worked hard to cut their own inventory risks so when a manufacturer finds an unexpected increase in demand, it can sometime take the primary market weeks if not months to react. The resulting shortages mean increased exposure to the secondary market and to the growing risk of counterfeit.

Global Growing Markets

A third macro trend in recent years has been the globalization of markets. Firms find themselves selling into new national and regional markets around the world, both as a consequence of expanding their targeted markets and of the rapid growth of the middle class in those developing economies. These newly established and emerging markets have introduced yet another layer of volatility into a company's forecasts and increased its exposure to shortages and the tide of fakes in the secondary market.

Electronics Everywhere

Magnifying the effect of growing markets has been the dramatic penetration of electronic components into entirely new products lines. A child's toy truck was once just bent metal with some plastic tires, but one now would be hard pressed to find a toy that comes without a dazzling array of flashing lights and sound effects. Automobiles will contain nearly twice the dollar value of electronic components in 2012 than they did a mere 5 years earlier. Newly electronic products mean even more volatility in the electronics supply chain.

Low Risk, High Return

Like smart businesspeople everywhere, criminals look to minimize risk and maximize their return on investment. In 2007, the US Federal Bureau of Investigation estimated that the distribution of counterfeit product was 900% more profitable than the distribution of cocaine. With narcotics smugglers facing mandatory sentences stretching into the decades, it comes as no surprise that criminal syndicates are attracted to selling counterfeit products, the penalty for which often amounts to just a few months behind bars.

<u>Specific</u>

Lack of Transparency

Criminals thrive in the dark, and one would be hard pressed to find a market with less transparency then the electronics secondary market. Serviced by brokers and independent distributors who make their profits by exploiting the information asymmetries between buyers and sellers, the components secondary market is built on a foundation of no transparency whatsoever. A broker would be foolish to identify his source to a buyer as they would be immediately cut out of any arrangement. With sometimes three or more brokers handling a component as it

makes its way through the market, there is ample opportunity for a knowing or unknowing broker to include fake parts in an otherwise legitimate shipment of goods.

Existing Filters Ineffective

Most brokers and independent distributors are well meaning, driven not just by altruism but also a dependence on the goodwill of their customers for future business. Manufacturer buyers will concentrate their spending on a handful of brokers in order to ensure the broker has a great deal to lose should counterfeit parts make it to the manufacturer. In years past, this reliance on brokers to weed out fakes has been an effective method for protecting the supply chain, but as the fakes themselves have become more sophisticated and advanced, the ability of the brokers to detect and remove them has fallen precipitously.

Even the most motivated broker employing best-practices often cannot identify which parts are legitimate and which are not. We have passed the point where traditional secondary market distributors are capable of protecting their customers from counterfeit electronic components.

Flavors of Fraud

Counterfeit components can take many forms, as criminals exploit the latest weakness in manufacturers' defenses. Quality inspections may adapt and deploy new tests to filter out fake parts, but the counterfeiters will always remain a step ahead. Companies may spend months improving their inspection processes, but counterfeiters can deploy new techniques within weeks, or even days. Given the substantial financial incentives at stake, counterfeiters will throw resources at hacking a firm's defenses by almost any means necessary, be that by redesigning a fake part's manufacturing or simply bribing a junior employee for access to the plant.

Fakes may come in many shapes and sizes, but at the simplest level, there are only a few different ways to misrepresent a component's authenticity: outright knock-offs, refurbished parts, mislabeled parts, and scrap. Some corner cases, such as intentionally malicious parts, are unique to products related to national security and are beyond the scope of this paper. Likewise, comprehensive detailed forensic analyses can be found elsewhere.

Knock-Off's
Outright knock-offs used to be the easiest to spot: poorly printed logos, misspelled names, and incorrect fonts. Just like fake watches are no longer humorously weak attempts to mimic a genuine Rolex, many component knockoffs look very much like the real thing. In fact, some plant managers have been known to run a "ghost shift". Occurring late at night when legitimate employees have gone home, ghost shifts use the same equipment and packaging as legit ones do, but will substitute inferior grade materials into the manufacturing process.

Refurbished Parts
Criminal elements, both inside and outside the secondary market, can make extremely large profits by purchasing discarded circuit boards and "pulling" certain high value components to resell. The process for removing these components from the circuit board and preparing them for resale includes direct exposure to extreme heat in loosening the solder, the physical stress of being tugged off the board, and the multiple strains of exposure to the hot oil used to clean off the last parts of solder. A little polishing and straightening of bent leads can make an old component look almost like new.

Mislabeled
The easiest technique a criminal can use is to falsify the documentation describing what a part is. Besides simply printing a meaningless 'certificate of compliance', counterfeiters can print a false label on the outside of a reel, tray, or tube, or they can alter the labeling on the surface of the component itself. Almost as soon as it was implemented, the European Union's Restriction on Hazardous Substances (RoHS) became a golden opportunity for counterfeiters who discovered that simply by relabeling the package in which components were stored, they could increase the resale value of those parts many times over.

Speed-steps, false RoHS status, modified part numbers and inaccurate certificates of traceability and compliance are perhaps some of the easiest and most profitable methods of misrepresenting a part.

'Scrap'
Component manufacturers need to pay special heed to their disposal partners as it is a frequent occurrence that components rejected at the fabrication facility for

subtle quality defects can be diverted from the scrap yard and find their way into brokers' hands and then into the legitimate supply chain. Given that these are legitimate components manufactured and packed at the legitimate facility, they can pose a special risk to their brand owners. Component makers should take extra precautions to ensure that every quality-rejected component is accounted for and certified as destroyed. Many firms will employ webcams and onsite personnel to monitor this process, though a low wage worker overseeing a scrap process could very easily be swayed with bribes.

Defending the Supply Chain

Given all these threats, how can a supply chain manager protect his company and his customers from the risk of counterfeit components? Using most of these approaches, it is impossible, but companies still have to try. Here is a high-level list of some of the different classes of defenses.

Buffer Stock

The easiest but most expensive way to avoid shortages is to maintain higher inventory levels, but the large measurable costs of maintaining high component inventory levels across the board far outstrip the likely cost of a shortage in one particular component. Managers have made huge strides in recent years in transforming their supply chains to a lean environment, and perhaps the costs of shortages can be used to justify the maintenance of a larger buffer stock, but given both the uncertain and imprecise costs of shortage and the very large and easily measureable cost of maintaining excess, most organizations would have a difficult time in building support for such a measure.

Buy from Franchise

As franchised distributors will rightly observe at every opportunity, the best way to protect against counterfeit parts is to purchase direct from authorized channels. Unfortunately, if a manufacturer can find parts from their primary market suppliers, it does not have a shortage, by definition. Companies with shortages have presumably exhausted their authorized channels and must turn to the grey market for supply. The franchised distributors are correct that avoiding the uncontrolled grey market will protect companies from counterfeit, but urging buyers to 'buy from franchise' will not protect them.

Visual Inspections

One of the key services brokers and independents play is to protect their end buyers by filtering out bad or unreliable parts. In recent years, their effectiveness as a filter has been called into question as counterfeiters have improved their technique markedly. With manufacturing relocating to China and other low-cost manufacturing regions with weak intellectual property protections, counterfeiters have gained access to the same technologies and equipment that legitimate manufacturers use themselves. As noted above, fake parts increasingly look like the genuine article, and secondary market intermediaries are proving incapable of detecting and, therefore, filtering out these fakes.

Component Testing

As counterfeiters have gained access to better technologies, not only do their wares look like the genuine article but they perform as well as the real product…for a while. Fakes nowadays will often pass initially quality tests, but because they lack the durability to hold up in 'real world' conditions, will fail later on, after it has passed quality checks. Just like any quality defect, the costs of counterfeit parts increase exponentially as the item advances further along the manufacturing process. Furthermore, the quality team faces a tough question: which parts to test? Criminals are smart enough to spread their fake parts out along a reel or to scatter them throughout a tray or pallet. Even if a part passes a test, there is no assurance that the items to its left and right are legitimate.

Trackability/Traceability

The primary market has a high level of accountability, visibility and control. When an item moves through the primary supply chain, it is possible to identify where that part has come from and where it is going. No such ability exists in the secondary market, where brokers and independent distributors are able to make money precisely because there is no information available to buyers or sellers that tells them how to connect. Creating trackability and traceability is simply not feasible with the grey market business model.

Enhanced Supplier Screening

Some purchasing departments place great faith in their abilities to evaluate grey market suppliers for their trustworthiness. Procurement managers insist on certifications, facility inspections, audits and strict internal processes from brokers

who wish to earn a spot on their approved vendor list. Due to the very nature of the grey market, where some 80% or more of orders are brokered between two or more middlemen, the truth is a buyer really has no visibility into where companies on the AVL purchased the components. There is little point vetting your immediate supplier without visibility into who their suppliers are.

Policing of Secondary Market

Many component manufacturers will hire investigators to police the secondary market to find counterfeit parts and report the vendors to local authorities. Even the most robust efforts are a mere drop in the ocean and are intended strictly as deterrence to the next group considering knocking off a manufacturer's brand. Other component makers install elaborate authentication technologies in their product, but such tools require expensive infrastructure and training to use. While employing these brand protection measures may be desirable from the upstream component maker's perspective, they do not measurable change the counterfeit risk profile for the downstream manufacturer who faces potential shortages across their entire bill of materials, not just one or two parts.

Government Regulation

Governments have becomes very active in drafting anti-counterfeiting laws and regulations, but because supply chains are so uncontrolled, these measures do not materially change the risk profile for a would-be counterfeiter. Governmental action is important, but, like governmental efforts to stamp out the drug trade, its effectiveness is uncertain, at best.

Inspections & Police Action

Like other corporate and government efforts to crack down on counterfeiters, raids and inspections are severely limited in their ability to protect the supply chain. They may act as a deterrent to some weak-willed criminals, but most criminals will simply chalk the occasional seizure as the cost of doing business. The FBI estimated that distributing counterfeit product was nine times more profitable than distributing cocaine – with such extraordinary profit margins, it is highly unlikely that counterfeiting gangs will abandon their efforts easily.

Supply Chain Pedigree

As Verical sees it, the only way to truly protect the supply chain from the risks of counterfeit components is to redesign the marketplace serving shortage buyers. Instead of permitting excess inventory to slide into the grey market, where it loses its traceability, Verical maintains inventory in an 'extended primary market', where manufacturers enjoy similar levels of visibility and control that they do elsewhere in the primary market. By enabling firms with excess components to market them directly to buyers in the secure and controlled environment, Verical ensures a safe and reliable stock of inventory and gives buyers the confidence they need to make good decisions sooner.

Conclusion

The threat of counterfeit components has never been greater. Counterfeiting is too profitable and too easy to stop. The high tech supply chain has never been more vulnerable, and the costs of counterfeit have never been so high.

Every time legitimate supply chains adopt a new approach to stop fakes, the criminal will adapt and defeat them. Markings, labels, testing – all of these are just temporary defenses against highly motivated and well financed criminal syndicates. In the endless arms race of authentication and counterfeit, the counterfeiters will always win.

Visual inspections may slow counterfeiters temporarily, but the criminals will always adapt and become even more sophisticated. The only defense that counterfeiters cannot defeat is one based on the one thing they cannot replicate: supply chain pedigree. A part's chain of custody resides in the databases of the legitimate manufacturers and distributors of the world.

Author John P. Brown is co-founder and VP of Marketing and Strategy at Verical, an emerging online electronic components marketplace. He brings a wide range of experience in operations, supply chain, marketplace design and anti-counterfeiting. A term member of the Council on Foreign Relations, John focused on information management and infrastructure protection at the Department of Homeland Security and holds a BA, MPA and an MBA from Harvard. Learn more about Verical at http://www.verical.com/, blog: http://blog.verical.com, Twitter: @Verical, and email John at jbrown@verical.com.

Please feel free to publish the above commentary in full or in part with attribution according to the Creative Common license.