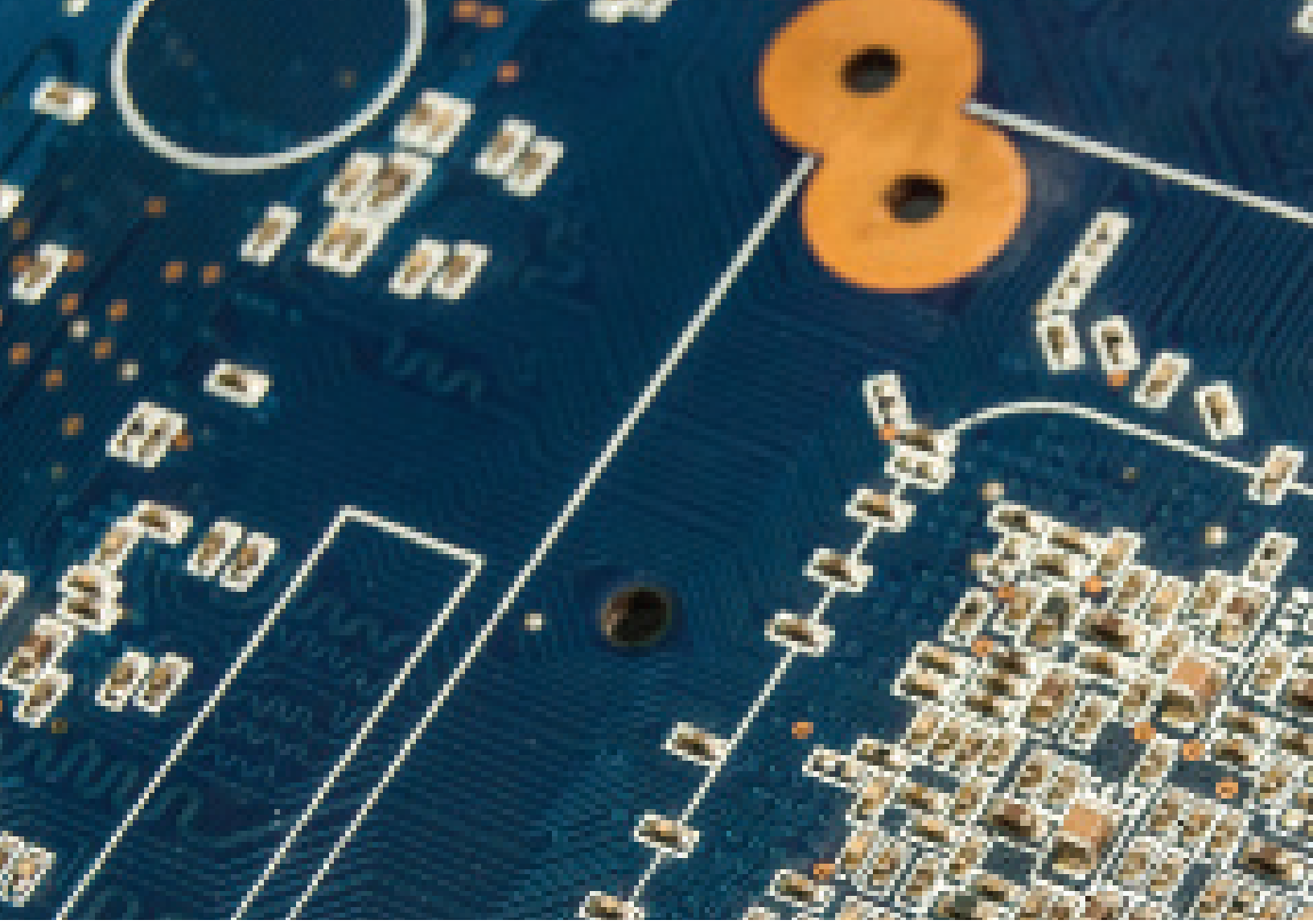
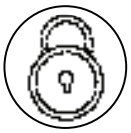


COUNTERFEITING: THE RISING THREAT TO ELECTRONICS MANUFACTURERS

A LOFTWARE WHITE PAPER BY JOE LONGO

WHITE PAPER

LOFTWARE
ENTERPRISE LABELING SOLUTIONS



COUNTERFEITING: THE RISING THREAT TO ELECTRONICS MANUFACTURERS

A LOFTWARE WHITE PAPER BY JOE LONGO

WHITE PAPER

Executive Summary

As a serious challenge to today's global electronics supply chain, counterfeiting and gray market diversion of electronics components threaten the integrity of products for manufacturers. Counterfeits and obsolete electronics components contribute to dangerous business exposure for manufacturer's customers, and compromise health and safety for consumers. Clearly, new solutions are needed to improve electronics supply chain integrity and stability.

Although unit item serialization[1] is one of the most powerful anti-counterfeiting and anti-diversion measures available today, many manufacturers lack standardized, automated, enterprise-wide labeling solutions as a foundation upon which serialization can be implemented efficiently and cost effectively. This is because many large electronics organizations, their suppliers, and their distributors still rely on a mish mash of 3rd party and homegrown barcode labeling systems. Serialization technology cannot be applied consistently or affordably throughout a non-standardized labeling environment.

However, Enterprise Labeling Solutions can provide the first line of defense in today's complex high technology electronics distribution environment. Enterprise Labeling offers a dynamic and data-driven approach for the creation of complex 1 and 2D barcode labels. It provides a platform for standardization, automation, scalability, and efficient maintenance while allowing businesses to react quickly to evolving customer, regional and regulatory requirements, and ensures consistency across a global supply chain. Enterprise Labeling Solutions enable electronics manufacturers, suppliers, and vendors to meet performance and scalability requirements with power and flexibility. Then when a company is ready to add unit item serialization technology as an additional powerful deterrent to counterfeiting and diversion, unique product identifier serial numbers can be integrated with minimal disruption and effort. Now is the time for all responsible electronics supply chain stakeholders to look to Enterprise Labeling Solutions as the best rapid response strategy to one of the most critical supply chain challenges today.

[1] Serialization technology provides a means by which products can be uniquely identified with a serial number at the unit item level, as opposed to lot or batch levels. The individual item, such as a circuit board, battery, etc., is assigned with a unique serial number that is embedded in a 1D or 2D barcode, or other type of tag, including RFID tags, human readable numbers, holograms, and other covert identifying methodologies.

LOFTWARE ENTERPRISE LABELING SOLUTIONS

©2015 Loftware, Inc. All Rights Reserved. All other marks are the property of their respective owners. • www.loftware.com

Counterfeits Jeopardize Lives and Cost Billions

Examining the electronics global supply chain landscape, the critical nature of the problem of counterfeits and obsolete products is sobering.

The public has heard rumors about the serious problem of electronics counterfeits for many years, but the magnitude and complexity of the challenges have only come into sharp focus over the last ten years, and in the last five years in particular. For aerospace, military, and other high tech industries, the discovery of counterfeits has ignited intense debate over how to lessen the alarming risks involved. Without a doubt, counterfeits or obsolete components can, sooner or later, fail to perform under critical circumstances. There are a number of factors which have contributed to the difficulty in understanding what to do about obsolete and counterfeit electronics, not the least of which has been the lack of visibility of components as they travel through the supply chain.

Many experts insist that the high prevalence of electronic counterfeits has arisen as a bi-product of the gray market, which is the unauthorized sale of new, branded products diverted from mainstream distribution channels. Some estimates state that up to 8% of total market revenue for electronics components are diverted through the gray market. For the semiconductor industry alone, which earned almost $336 billion in 2014, the gray market could account for up to $26.8 billion. The gray market has spawned a fraudulent and unreliable distribution system based on a marketplace clamoring for price discounts and high availability for more and more technology products. Counterfeits have crept into the gray distribution networks through rogue component design houses fronting as manufacturers, which then sell those products to independent distributors, who in turn ask the design firms to buy their products of choice from an authorized manufacturer. After distributors obtain these products illegally, components enter the gray market, are sold at sharp discounts over the Internet, and are often offered alongside counterfeit components, making it difficult to know which products are authentic and which are not.

The “underground” supply chain also handles obsolete parts found in e-waste[2] and used in remanufacturing. These obsolete parts have made their way into the hands of buyers who believe they are getting brand new products.

In this way, counterfeit and obsolete electronics have been discovered in missile guidance systems and hundred-million-dollar aircraft, causing serious security problems for the U.S. Department of Defense and its contractors. Who made these counterfeits, and are they programmed with malicious software from terrorist organizations designed to divert flights, radars or missile controls? What about tampering with commercial aircraft electronic components? What happens when an obsolete component fails? Certainly lives can be at risk.

There is understandably very little information about the sources of counterfeits. When investigative organizations divulge details of their findings, they are often obliged to protect their sources. Counterfeiters shut down and reopen regularly, mushrooming in multiple locations because they hear about sting operations through the media.

©2015 Loftware, Inc. All Rights Reserved. All other marks are the property of their respective owners. • www.loftware.com

So it is easy for manufacturers and suppliers to become discouraged with the risky gray market and counterfeiting environment today. What can be done about it? The U.S. Department of Defense finalized a new ruling in May of 2014 to detect and avoid counterfeit electronics[3] as an amendment to the 2012 National Defense Authorization Act, but many manufacturers are still not clear about who is responsible for which part of the ruling. The DOD has placed more of the responsibility on contractors to identify counterfeits, putting them in charge of the legitimacy of the supply chain to include their subcontractors and suppliers. How to meet that mandate, is the question.

"Military Grade" May Not Be Military Grade

One example of what can go wrong was revealed in the sting operation conducted by the government two years ago, called Operation Chain Reaction. U.S. Customs officials seized over 5.6 million electronic microprocessors destined for military contractors and the commercial aviation industry alone. A company called MVP Micro headquartered in Irvine, California profited by selling over 13,000 knockoff integrated circuit boards to over 420 buyers in the US and abroad. The U.S. Department of Justice sentenced MVP owner Mustafa Adbul Aljaff and former MVP operations manager Neil Felahy to 30 months in prison for conspiring to sell chips mislabeled "Military Grade." Although the monetary profit to the counterfeiter seems insignificant, had inspectors not been able to identify the counterfeits, those 13,000 integrated circuit boards, if faulty, could have amounted to untold value in damages to the military. In addition to the risk of loss of life, there are billions of dollars at stake.

According to a recent U.S. Senate committee report, "counterfeit electronic parts from China are flooding into critical U.S. military systems, including special operations helicopters and surveillance planes, and are putting the nation's troops at risk." The report specifically noted that Chinese companies take discarded electronic parts from other nations, remove any identifying marks, wash and refurbish them, and then re-sell them as brand new parts. All facets of the supply chain are now reporting instances of counterfeit products.

2 E-waste: Electronic waste or e-waste describes discarded electrical or electronic devices. Used electronics which are destined for reuse, resale, salvage, recycling or disposal are also considered as e-waste. (Wikipedia, the Free Encyclopedia, April 2015)

3Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012–D055; Final Rule, http://www.gpo.gov/fdsys/pkg/FR-2014-05-06/pdf/2014-10326.pdf

©2015 Loftware, Inc. All Rights Reserved. All other marks are the property of their respective owners. • www.loftware.com

Perfect Storm for Counterfeits Impacting Supply Chain

How did the electronics industry get to where it is now, at this critical juncture? The best answer for this surrounds the concept of market forces and the change in technology itself. Here are some events to consider:

- The Dot-Com bust – the massive investments in telecommunications and bandwidth made communication tools and services more available at a low-cost, bringing many new electronics businesses into the market.
- Outsourcing and off-shoring – the gradual shift of manufacturing away from USA and Europe to Asia made the visibility of counterfeit products more difficult.
- Windows widespread adoption - the interoperability of systems enabled users to share more information more readily and collect payment quickly.
- Inexpensive over-night shipping – the rise of FedEx, UPS, and DHL and their new offerings made it inexpensive to ship small packages.
- The growth of e-commerce making it easier for counterfeiters to sell goods anonymously.
- The recession of 2008 forced markets to seek out lower-cost supplies.
- China's entry into the World Trade Organization resulted in lifting the ban on non-government owned and controlled business entities.
- The Basel Convention of the early 1990s resulted in the USA exporting e-waste to the developing countries, primarily China, where e-waste recycling has become a way of life. Despite the toxic effects of e-waste; this has provided the valuable raw materials for today's counterfeiters.

How Are Counterfeits Identified Now?

So by what methodologies is the electronics industry identifying counterfeits? After all, it is not as easy as detecting a knock-off Louis Vuitton bag or a Rolex watch. A savvy consumer can often tell in a glance whether a designer hand-bag or a pair of shoes is genuine or not. But electronics counterfeits hide deep within products or systems, and are not easy to detect. Inspectors cannot open up every product to test components inside. The most obvious way to avoid counterfeits is to buy parts exclusively from authorized OEMs (Original Equipment Manufacturers). The National Defense Authorization Act uses this approach under Section 818, stipulating that all contractors and sub-contractors doing business with DOD must purchase their parts from authorized OEMs. But OEMs may have unknowingly included obsolete or counterfeit parts in their manufacturing process.

4The ESFi Organization (Electrical Safety Foundation International) surveyed over 900 electronics professionals including manufacturers, inspectors, contractors, and distributors, and 96% reported they consider counterfeits to be a substantial or moderate threat. One third of the respondents had found 5 or more counterfeits in their routine line of work in the previous year. Over one third said their companies do not have defined best practices for identifying counterfeits.

©2015 Loftware, Inc. All Rights Reserved. All other marks are the property of their respective owners. • www.loftware.com

Various technologies do offer partial solutions to the counterfeiting problem. Companies can scrutinize packages for signs that pins have been straightened or indications that labels have been sanded and repainted. They can also perform more detailed analyses using X-ray, scanning electron, or acoustic imaging to look inside a package for things that might be amiss, like the improper placement of a chip within its package. In addition, DNA, which adds forensic markers to products for the military, has been used on a limited basis.

Meanwhile, counterfeiters are getting better at their craft every day. They buy discarded components on the cheap and sell them at full retail price, then use those profits to get even better at hiding their components. Ethical distributors face competitive challenges since they buy and sell components at razor thin margins. Any testing just adds to their costs, and it is simply not practical for most companies that buy subsystems to test every component within them.

Through various means of detection, here are just a few examples of the serious nature of counterfeits identified and reported to the public recently by the U.S. National Intellectual Property Rights Coordination Center:

The purchase of counterfeit Cisco converters by an individual, who intended to sell them to the DoD for use by the Marine Corps to transmit troop movements, rely intelligence and maintain security for a military base.

A global procurement and distribution network, based in California, provided counterfeit integrated circuits to various governmental agencies, including the military and prime DoD contractors. Agents conducted undercover purchases from individuals within the company under official navy contracts and were provided counterfeits for various weapon platforms.

A Florida-based electronics broker providing counterfeit integrated circuits to a prime DoD contractor fulfilling a Navy contract for components destined for implementation into ship and land based antennas.

What About the Commercial Supply Chain?

And while the military detects a good percentage of counterfeit parts coming into their sphere of purchases, the commercial side is still wide open. Counterfeiters view the commercial supply chain as much more attractive. The commercial market is much larger and more diversified, the level of testing is lower, and product life cycles are much shorter.

This gives counterfeit parts more time to hide and counterfeiters more time to sell their wares.
The notion of a commercial supply chain laden with counterfeit parts is truly sobering. Counterfeit parts have been found in servers, routers, storage hardware, and other electronics systems. These systems enable communications, transportation, power, and critical infrastructure to run our daily lives.

©2015 Loftware, Inc. All Rights Reserved. All other marks are the property of their respective owners. • www.loftware.com

For example, here is a list of some of the electronic products under FDA jurisdiction:

- Television receivers
- Computer monitors
- X-ray machines (including medical, research, industrial, and educational)
- Electron microscopes
- Black light sources
- Welding equipment
- Alarm systems
- Microwave ovens (devices that generate microwave power)
- All lasers (including low power lasers such as DVD and CD readers/writers/players) and other light emitting devices (Infrared and Ultraviolet)
- Ultrasonic instrument cleaners
- Ultrasound machines
- Ranging and detection equipment, such as laser levels

Unfortunately, most solutions today only detect counterfeit components after they enter the supply chain, not before they enter the supply chain. Unethical suppliers need to be identified and shut down because they manage to stay in business today--even proliferate--because there are no consequences for their actions. Better technologies are needed to track parts as they move through the supply chain, so that data can be shared with the industry at large to discredit unethical suppliers.

Some additional methods companies are using to detect counterfeit electronics include:

- Indentation & Marks
- Decapsulation
- Electrical Inspection
- X-Ray and SEM Inspection

©2015 Loftware, Inc. All Rights Reserved. All other marks are the property of their respective owners. • www.loftware.com

Serialization: Getting Ready for a Powerful Solution

Another powerful technology that is in a relatively early stage of acceptance is serialization. Unique serial numbers are designated to each and every product through complex algorithms that originate from a separate database integrated with the manufacturer's production line. Serial numbers follow the product as it moves along the supply chain so it can be reliably traced back to the source. This form of Mother–Daughter serial number relationship provides a quick way to determine if the source is valid before it gets to its final destination–the customer. The serial number, which is a unique identification number similar to an automobile's VIN number, can be checked against a database to verify the product's authenticity from its origin. These numbers are extremely difficult, if not impossible, for counterfeiters to duplicate.

Considering the number of stops a normal package makes along the supply chain, serialization gives manufacturers, distributors and shippers a much higher rate of confidence in the integrity of their electronic components.
A combination of all these security methods is often employed, and together with serialization technology, a hybrid approach can be a powerful protective solution, with serialization as one of the most advanced. However, most manufacturers are ill prepared to institute a serialization-based track-and-trace system. Serialization is challenging to implement unless electronics supply chains have a standardized, robust, and automated labeling solution in the first place.

Enterprise Labeling Solutions: The First Line of Defense

In addition to the important question of authenticity, today's electronics product labeling requires a variety of complex information with data integrated from a large number of data sources. Varied labeling governmental regulations and standards for new and existing markets, the need for speed due to new automation technologies in manufacturing, requirements for multiple languages, complex barcode data, and more—the real estate on a single label is populated with data from a variety of repositories. But many large companies are not managing this level of complexity with a reliable labeling strategy sophisticated enough to cover all these needs. It is understandable, then, that an attempt to serialize at the unit item level is putting the cart before the horse for many organizations.

Also, for affordable and effectively manageable security measures to be implemented in the supply chain, the ability to allow approved electronics supply chain suppliers and distributors to participate through a streamlined labeling solution is required. This secure access by authorized supply chain participants is the "first line of defense" against counterfeiting and diversion. Standardization of barcode labeling solutions with approved suppliers and distributors can greatly diminish the likelihood of obsolete or counterfeit components making their way into the supply chain. Enterprise Labeling Solutions allow for secure access by approved suppliers and partners, as well as offer many other benefits to manufacturers. Enterprise Labeling prevents mislabeling through automation while offering support for regulatory data, multiple languages, and customer specific labeling requirements. In the end, labeling consistency and reliability are exponentially improved.

©2015 Loftware, Inc. All Rights Reserved. All other marks are the property of their respective owners. • www.loftware.com

With serialization technology added to Enterprise Labeling Solutions, an unprecedented degree of security in tracking electronics components can save billions of dollars and prevent other human and environmental disasters.

The complexity of today's labeling requirements point to the fact that without the solid foundation of a good labeling strategy, customer dissatisfaction, returned shipments, counterfeits, and loss of business can accumulate, leading to significant erosion of revenue and profitability. Most importantly, the dangers of counterfeiting and diversion can include a negative impact on human health or even contribute to loss of life.

The Electronics Industry is in an exciting phase of rapid expansion and change, and outdated labeling solutions are unable to keep pace with these dynamics. Fortunately, Enterprise Labeling is one immediate way the electronics industry can take charge in response to this changing environment, be more responsive to the critical nature of the current labeling challenges, and improve the stability of global supply chains while concurrently stemming the dangerous rising tide of counterfeits.

About the Author
Joe Longo is Electronics Industry Specialist with Loftware and has been working with Loftware enterprise customers in the electronics industry for over seven years. His customers include some of the largest electronics manufacturers in the world: Jabil Circuits, Flextronics, Celestica, Kemet, Plexus, GE and more. Highly knowledgeable about the key issues most EMS manufacturers are facing today, he provides in-depth studies and recommendations to electronics manufacturers on solutions to their labeling requirements.
Email: jlongo@loftware.com.

About Loftware
Loftware, Inc. is the global market leader in Enterprise Labeling Solutions with more than 5,000 customers in over 100 countries. Offering the industry's most comprehensive labeling solution, Loftware's enterprise software integrates SAP®, Oracle® and other enteprise applcations to produce mission-critical barcode labels, documents, and RFID Smart tags across the supply chain. Loftware's design, native print, and built-in business rules functionality drives topline revenue, increases customer satisfaction, and maximizes supply chain efficiency for customers. With over 25 years of industry leadership, Loftware's Enterprise Labeling Solutions and best practices enable leading companies to meet their customer specific and regulatory requirements with unprecedented speed and agility. Loftware, with hundreds of electronics industry customers worldwide, is the foremost authority and global market software leader in delivering innovative business solutions for enterprise labeling requirements. Visit www.loftware.com.

©2015 Loftware, Inc. All Rights Reserved. All other marks are the property of their respective owners. • www.loftware.com