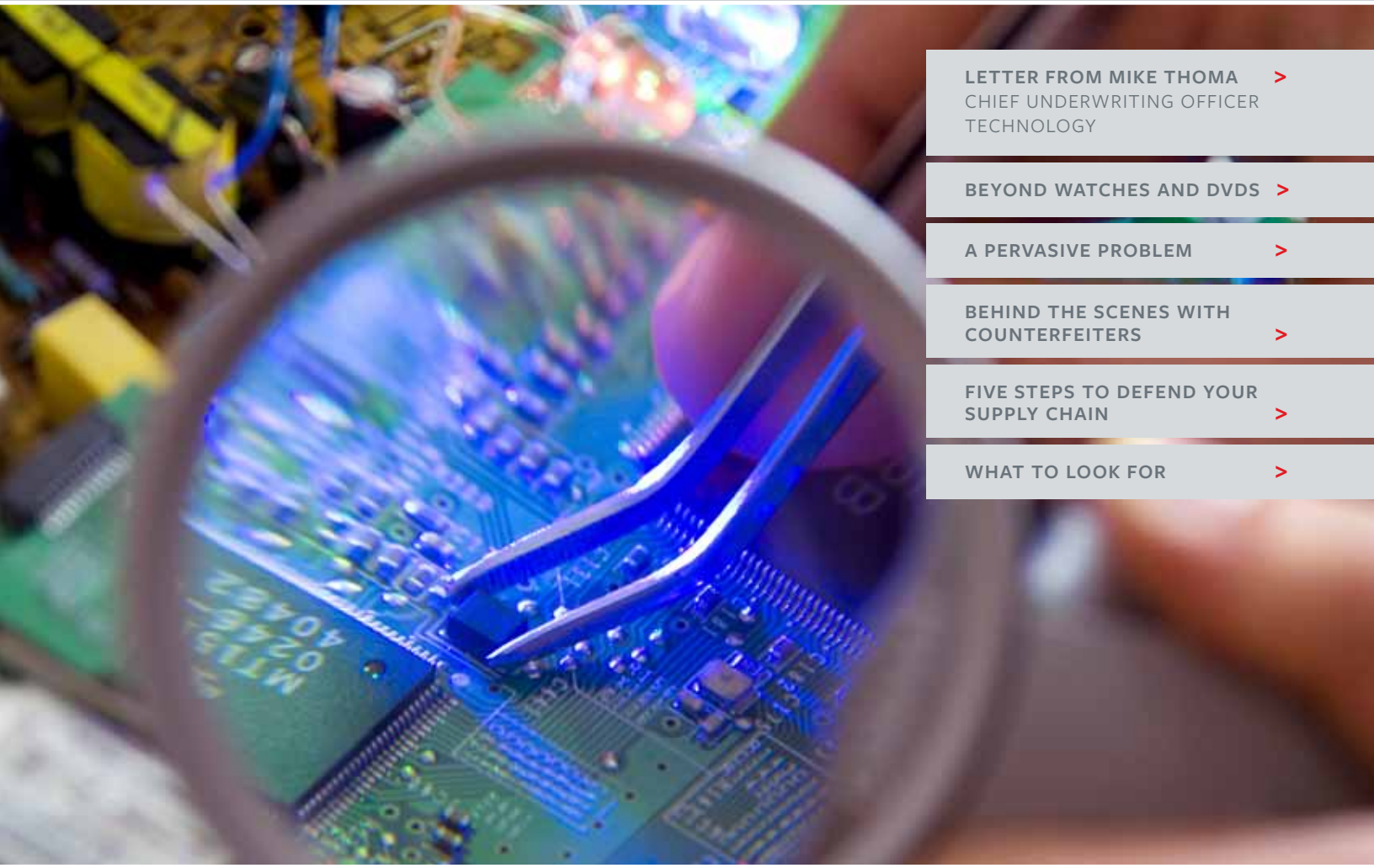


TRAVELERS

Getting Real

DEFENDING YOUR SUPPLY CHAIN FROM COUNTERFEIT COMPONENTS
HELPING COMPANIES MANAGE RISK

Risk Advisers: Emerging risk issues brought to the fore front

A troubling increase in counterfeit components means many industries are at risk for delivering imperfect products or faulty services. Whether it's a medical device firm counting on sophisticated components to safeguard a patient's health, a manufacturer delivering finished products to eager customers, or a transit system ordering an automated safety system, no business can afford the damage and liability that can be caused by undetected counterfeit parts. Unfortunately, distinguishing real parts from fake ones is not always easy.

In this article, we discuss:

- The various forms of counterfeiting
- The scope of the problem as indicated by government reports and industry estimates
- Steps companies can take to protect themselves and their customers

Our author, Marlyn Cain, underwriting director of electronics manufacturing, is responsible for development and implementation of strategic underwriting for the electronics manufacturing industry. Marlyn is a well-regarded resource. I encourage our readers to reach out to her at mcain@travelers.com or 651.310.5308.

— *Mike Thoma*
Chief Underwriting Officer of Global Technology at Travelers

Beyond watches and DVDs

Most people know that if they buy a "designer" purse or watch from a street vendor at a stunningly low price, they're actually getting an imitation product that only resembles the luxury goods with famous names. Similarly, inexpensive DVDs are often pirated versions that have nothing to do with the studios and distributors that market post-theater-run movies.

These counterfeit items infringe on the rights of those who developed the original products, and the economic injury may be substantial. Nonetheless, these imitations are not likely to physically harm anyone or cause a company to face a product liability lawsuit.

Such is not the case with counterfeit components. For example, electronic parts that many industries import from overseas and rely upon for their finished goods may pose significant risks for the importing company. A counterfeit part may cause a product to either stop working or malfunction in a way that could potentially cause harm to human life.

Of course, no company sets out to buy fake parts. When a company purchases electronic components, it requires – and expects – the parts to meet specifications that make them suitable for use. This may include materials expected to hold up over time, be built with precision that will ensure proper operation, and be free of defects that could cause malfunctions.

However, the seller may claim a component meets the specifications of the buyer when, in fact, it does not. It may be made from inferior or refurbished materials, or made by a non-compliant manufacturer who is not following industry standards for producing the component.

In addition, a component could be a reject from a legitimate manufacturer's quality-control process, slightly modified in some way and sold as a high-quality product.

If the components include hazardous substances that are regulated by some governments, such as the European Union's restrictions on mercury, lead or cadmium, other forms of fraud may come into play. For example, the part may be accompanied by false certification of environmental or regulatory compliance.

While a part may be counterfeit in any number of ways, the impact on the company purchasing the part generally falls into two categories:

Non-functional parts

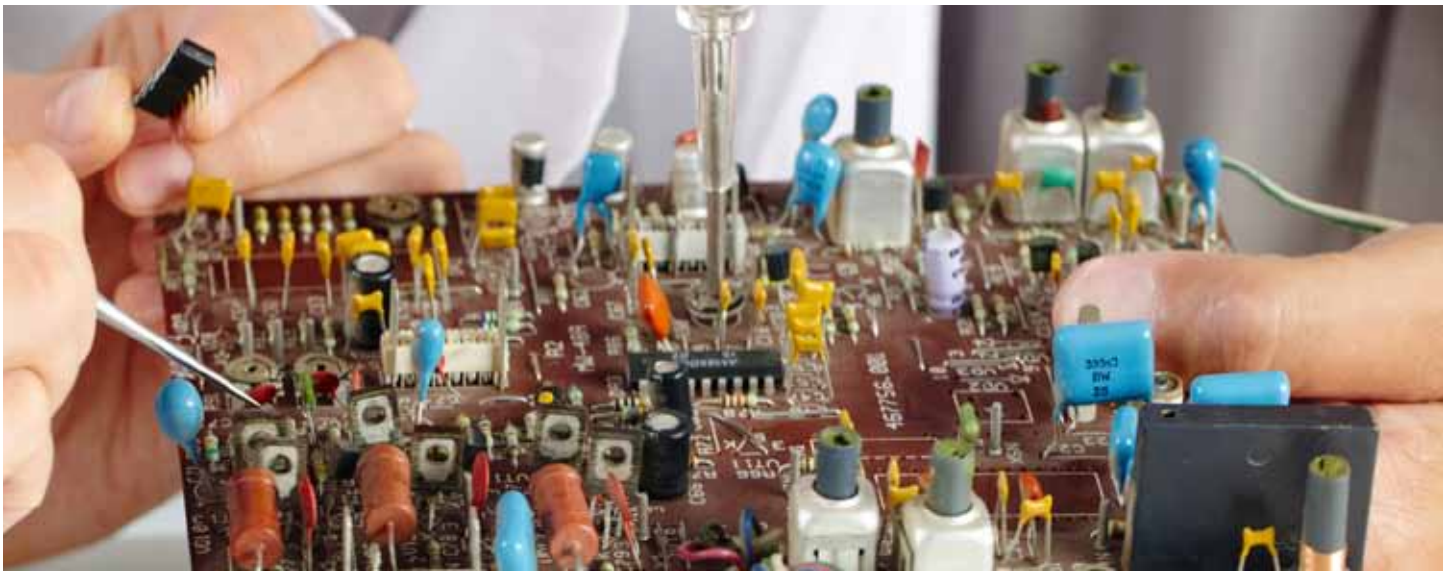
These components arrive at the buyer's facility appearing legitimate but when they are incorporated into products, there are immediate problems because they do not work as expected. While this can cause delays in manufacturing, the products are unlikely to make it to the market and into consumers' hands because the buyer will quickly discover them to be non-functional.

Functional substandard parts

In this scenario, the components work as expected. However, they may be refurbished devices with short operating lives or devices made out of substandard materials that may quickly deteriorate after being put to use by the end user. These can expose a company to liability.

A pervasive problem

No one is sure how prevalent counterfeit components are, but some experts believe up to one out of every 10 technology products worldwide are not what they seem to be. The Federal Aviation Administration estimates that 2 percent of all electronic components installed in aircraft are counterfeit. And *Businessweek* called counterfeit electronic components a $10 billion business in 2008.



"Counterfeit parts – generally the misrepresentation of parts' identity or pedigree – can seriously disrupt the Department of Defense supply chain, harm weapon systems integrity, and endanger troops' lives," stated the GAO report.

And the problem appears to be growing. Research firm IHS, which tracks counterfeit parts documented by the Government-Industry Data Exchange Program and other organizations, reports that incidents increased four-fold between 2009 and 2011. Similarly, the federal Department of Commerce's Bureau of Industry and Security found that incidents more than doubled from 2005 to 2008.

Perhaps the most telling indictment of suppliers who pass off counterfeit parts as real came in a 2012 Government Accountability Office (GAO) sting operation. All of the 16 parts the GAO ordered after selecting vendors based on low bids were judged to be "suspected counterfeit" by an independent testing lab. In fact, the GAO supplied bogus part numbers for four of the 16 items ordered, yet received products even though the parts do not exist (see next page for details of the GAO operation).

"Counterfeit parts – generally the misrepresentation of parts' identity or pedigree – can seriously disrupt the Department of Defense supply chain, harm weapon systems integrity, and endanger troops' lives," the GAO wrote in its report to the Senate Committee on Armed Services. However, the GAO warned that the sample was not sufficient to make generalizations about the extent of counterfeiting, and the report did not include recommendations.

Other organizations have been active in making recommendations, however. The Aerospace Industries Association issued a report in March 2011 that encouraged companies to take a number of steps, including better procurement standards and training, documentation and sharing of information about counterfeit part incidents, and the adoption of best practices in e-waste recycling to keep discarded parts out of the supply chain.

In addition, a number of organizations – including the Independent Distributors of Electronics Association (IDEA) and the U.S. Department of Defense – have issued, and are developing, further standards for evaluation of purchased components.

A closer look at GAO sting

What do military-grade component vendors do when they are faced with orders for difficult-to-supply parts? Apparently, some fake it.

As part of an experiment in obtaining military-grade components using specialized Internet purchasing platforms, GAO created a fictitious company and submitted requests for bids for 16 parts in three categories: authentic part numbers for some obsolete or rare parts, authentic part numbers with date codes after the last date the part was manufactured, and fictitious numbers not associated with any parts.

GAO received responses from 396 vendors, of which 334 were located in China, 25 in the United States and 37 in other countries. Selecting the lowest bids, GAO ended up making purchases only from vendors in China.

Writing about the results, GAO reported:

Specifically, all 12 of the parts received after GAO requested rare part numbers or post-production date codes were suspect counterfeit, according to the testing lab. Multiple authentication tests, ranging from inspection with electron microscopes to X-ray analysis, revealed that the parts had been re-marked to display the part numbers and manufacturer logos of authentic parts. Other features were found to be deficient from military standards, such as the metallic composition of certain pieces. For the parts requested using post-production date codes, the vendors also altered date markings to represent the parts as newer than when they were last manufactured, as verified by the parts' makers. Finally, after submitting requests for bogus parts using invalid part numbers, GAO purchased four parts from four vendors, which shows their willingness to supply parts that do not technically exist.

Making the grade

There are several widely recognized sources of standards that provide guidelines for industry-accepted quality criteria for electronic components. Among them are:

Independent Distributors of Electronics Association (IDEA) – IDEA-STD-1010, advice on establishing inspection procedures and full-color photographs of what components should look like. A related standard, IDEA-ICE-3000, is a professional inspector certification exam to demonstrate competency with the IDEA-1010 standard.

SAE International – AS5553 (Avoidance, Detection, Mitigation and Disposition), AS6171 (Test Methods Standard) and AS6081 (Avoidance Protocol).

Federal Defense Logistics Agency test method standards – Mil-Std 1580, Destructive Physical Analysis for Electric, Electromagnetic, and Electromechanical; Mil-Std 883, Microcircuits; Mil-Std 750, Semiconductor Devices; Mil-Std 202, Electronic and Electrical Component Parts; and Mil-Std 981, Design, Manufacturing and Quality Standards for Custom Electromagnetic Devices for Space Applications.

Behind the scenes with counterfeiters

Counterfeit components often begin their life as e-waste. While the original owners may think they have properly disposed of their e-waste so that rare metals and other materials can be reclaimed and reused, e-waste often ends up overseas where it is rapidly converted into "new" parts.

The April 2011 issue of Medical Electronics Design included an article entitled "Dodging Counterfeit Electronic Components Is Far More Difficult than in the Past," describing the difficulty of detecting counterfeit parts. The following excerpt is a description of how plastic-encapsulated microcircuits (PEMs) are harvested from used circuit boards, "refurbished" and sold as new.

In one case in particular, workers were heating printed circuit boards, one at a time, over small fires until the solder reflowed. The board was struck against a hard surface to make the components fall off, and the components were then gathered off the ground. The individual components were packed in bags, washed in streams and rivers, dried on sidewalks, sorted, and returned to the counterfeiter's workshop where the original part markings were sanded off.

The surface of each component was then painted to resemble the original component color and to cover sanding marks. After drying, the parts were re-marked, using an ink or laser-etch process.

All of this rough treatment would be damaging even to brand new components, never mind components that have already seen a lifetime of service. Aside from the fact that some of the components are unquestionably dead electronically at this point, a single pile may contain components having different revision codes, or even different functions. But every component in a pile will get the same new matching part marking.

Five steps to defend your supply chain

The key to ensuring that your company does not end up with counterfeit parts is to be aware of the issue in advance and take appropriate countermeasures. The following **five steps** can help you establish a procurement system that makes receiving fake components much less likely.

1. Know your seller

Don't just accept the lowest bid — if the price seems too good to be true, the components are probably counterfeit. Instead, try to always purchase from suppliers who are OEM-approved distributors. Check with others to see if they have had experience with a particular seller. Be cautious before placing your order.

2. Verify specifications

Make sure the specifications and documentation offered in a bid match exactly what you are looking for.

3. Trust, but audit

Once you have selected your vendor based on your background investigation and have established a relationship, be prepared to audit their performance over time. Make sure they do not switch to inferior supplies after you have been reassured by the first few shipments.

4. Perform quality control

Establish a system that is effective in screening out counterfeit parts. This should include a document review and visual inspection, and can also include one or more sophisticated techniques, such as electrical inspection, x-ray inspection, scanning acoustic microscopy and/or thermal analysis.

5. Adopt industry-approved standards

Adopt industry-approved standards. Review standards that have been set by organizations with expertise, such as the Independent Distributors of Electronics Association or the federal government, and decide which ones would be helpful in making your supply chain more secure.

Setting up an effective quality control system is probably one of the most important but challenging steps for a company to take. Such a system can begin with a simple inspection (see next page) but may also include a number of more rigorous processes. An electrical inspection, for instance, can be very basic and take only moments to determine if the component is functional. Or it may include a complex evaluation with multiple test fixtures and software to evaluate the component across a range of specifications.

The internal structure of a component can be viewed and compared to authentic parts by using X-ray equipment, X-ray Fluorescence (XRF), a Scanning Electron Microscope (SEM) or Energy Dispersive Electron Spectroscopy (EDS). The EDS equipment can help determine if a product is made of the right materials, such as gold rather than aluminum, and if it is compliant with lead-free specifications. Thermal analysis can also be used to compare parts.

Other equipment can detect alterations. For example, Fourier Transform Infrared Spectroscopy (FTIR) can detect the organic compounds that blacktopping agents (i.e. sanding or remarking counterfeit parts) are often made of, and Ion Chromatography (IC) can detect ionic contamination, such as salts and organic acids that are left behind during the counterfeiting process. Scanning Acoustic Microscopy (SAM) is a form of ultrasound that can detect evidence of relabeling, or can show density differences when compared to authentic components.

What to look for

A component may look exactly like you were expecting it to look, but still be counterfeit. Here are a few things to check for:

- Does the artwork on the component match the OEM-defined artwork such as color and markings?
- Are there sanding marks that indicate someone has removed old markings and replaced them with different ones?
- Is the artwork easily removed? Use three parts of mineral spirits to one part isopropyl alcohol. If the artwork comes off, it undoubtedly has been added by a counterfeiter.
- Has a polymer filler been used to make the exterior look right after a sanding and remarking process? Called blacktopping, this can be checked for with acetone. If the acetone removes the "surface" of the component, it is because blacktopping material was used to cover the counterfeiter's tracks. A sharp blade can also be used to test for blacktopping; you should not be able to scrape away the surface material from a real component.
- Are the leads bent or re-plated, the markings fuzzy, or is there some alteration of features that does not look crisp and well-defined? The use of an optical microscope can turn up many subtle flaws that are indicators of counterfeit parts.

Keeping it real

Businesses need to know that their reputation is on the line whenever they sell products or provide services to their customers. Additionally, there may be exposure to liability if the customer gets something other than they expected. With the proliferation of counterfeit components, it pays for each company to follow a best-practices approach to defend its supply chain.

ADDITIONAL RESOURCES

GAO investigation of counterfeit parts

http://www.gao.gov/assets/590/588736.pdf

Aerospace Industries Association report: Counterfeit Parts: Increasing Awareness and Developing Countermeasures, written December 2010, issued March 2011

http://www.aia-aerospace.org/assets/counterfeit-web11.pdf

For more information or to download our other Risk Advisor briefs, please visit Emerging Risks at https://www.travelers.com/business-insurance/specialized-industries/technology/emerging-risk.aspx

TRAVELERS

travelers.com