

Fighting a Flood of Counterfeit Tech Products

As distributors hunt for fakes, an "epidemic" of bogus chips, routers, and computers costs the electronics industry up to \$100 billion annually

By [Rachael King](#)

Edward Dimmler dips a cotton swab in acetone and rubs it on the surface of a computer chip that was ostensibly manufactured by [Samsung](#). The white tip turns black—the first clue that the part may be fake. Dimmler, director of warehouse operations at electronics distributor PCX, then inspects the chip under a microscope and sees the word Samsung smeared across the top of the chip. Clearly, this memory chip is counterfeit, ineligible for resale. Dimmler quarantines it in the bowels of his warehouse on one of the shelves painted red to denote knockoffs of well-known brands, including Intel ([INTC](#)), Advanced Micro Devices ([AMD](#)), and [NEC](#). "We now have to question everything," he says in an interview at PCX headquarters in Huntington Beach, Calif. "A part is considered suspect until we prove otherwise."

In the past five years, counterfeit computer chips, routers, and other electronic products have "become an epidemic," says PCX Chief Executive Gil Aouizerat. The number of counterfeit electronic products uncovered in the defense industry alone more than doubled in 2008 to 9,356, from 3,868 in 2005, according to a January 2010 report by the Commerce Dept. Fake gear costs the information technology industry an estimated \$100 billion a year, according to the National Electronics Distributors Assn.

A counterfeit product is typically less reliable than the real thing, if it works at all. Fakes can impede tasks as varied as automotive navigation, medicine dispensing, and intelligence gathering. In January, Ehab Ali Ashoor, a Saudi citizen who lives in Sugar Land, Tex., was convicted of purchasing and selling counterfeit Cisco Systems ([CSCO](#)) parts intended for use by the Marine Corps. to monitor troop movement, relay intelligence, and maintain base security in Iraq, according to the Justice Dept. "Counterfeiting is a very serious issue that impacts the entire high-tech industry on a global level, and Cisco and other leading IT companies have been actively addressing this issue for several years now," says Cisco spokesperson Kristin Carvell.

In 2007, a malfunctioning router used by U.S. Customs and Border Protection at the Los Angeles International Airport resulted in delays for 17,000 passengers, according to the Homeland Security Dept. The problem was caused by a counterfeit version of a component designed to aid communications with the network, says Peter Hlavnicka, treasurer at the Alliance for Gray Market and Counterfeit Abatement. The anticounterfeit organization was formed in 2001 by 3Com ([COMS](#)), Cisco Systems, Hewlett-Packard ([HPQ](#)), Nortel, and Xerox ([XRX](#)).

Bogus parts in authorized channels?

[China is the source of many counterfeit electronics](#) coming into the U.S., according to a January report by the Commerce Dept. In many cases, parts are harvested from electronic waste sent to

China for recycling. For instance, workers dismantle motherboards, recover components, and sand the parts to remove markings. They then imprint forged dates, brand names, and product codes. The parts make their way to electronics marketplaces and other intermediaries before being distributed globally by suppliers. Other countries atop the Commerce Dept.'s list are Taiwan, Singapore, and Malaysia.

Counterfeit components may even be infiltrating authorized channels. Andrew "bunnie" Huang is an engineer at [Chumby Industries](#), maker of Internet-connected alarm clocks. While at work on one of Chumby's products in December, Huang found a batch of suspect Kingston memory cards, he wrote in a detailed Feb. 16 [blog entry](#). All had come from the same authorized Kingston dealer, which claimed the cards were authentic but ultimately provided a refund. The construction of the cards in question "is similar to another card of clearly questionable quality, which leads me to question Kingston's judgment in picking authorized manufacturing partners," Huang says.

In January, Kingston began shipping memory products with anticounterfeit labels to better prevent fakes from being sold as authentic products, the company said in February, although it didn't say its actions were connected to Huang's discovery. Kingston spokesman David Leong declined to comment.

Would-be victims are banding together. The Defense Dept. and the National Aeronautics and Space Administration have helped create standards that they hope will help users avoid buying counterfeit parts, says Debra Eggeman, general manager of Independent Distributors of Electronics Assn., a trade organization that teaches members how to detect counterfeit products. Blacklisting is a common remedy when distributors are found to have sold counterfeit parts.

shavings can foil the acetone test

Finding fakes isn't always easy. At PCX headquarters, Dimmler displays what looks like a movie reel, but which consists of a string of about 1,000 tiny chips. Then he pulls out a quart-size bag containing countless chips no larger than flakes of finely ground pepper—so small they need to be viewed under high-powered microscopes. To an untrained eye, the components all look real. To examine them, Dimmler inspects such minutiae as logo placement, the tightness of vacuum-package sealing, and the depth of etchings on a chip's face.

Complicating matters, counterfeiters are growing more adept at disguising their handiwork. For instance, some save the shavings from original, valid chips and then blend them into coatings for fakes to prevent the acetone test from uncovering fraud.

Global IC Trading Group, an independent distributor that buys and sells electronic components, including memory, processors, and integrated circuits, has invested in high-tech equipment to test components as they come through its Laguna Hills, Calif., operation. In addition to

conducting physical inspections and swabbing products with alcohol or acetone, the company X-rays components and de-encapsulates them to inspect the interior die for markings and dates. "We've probably invested about a quarter of a million dollars in less than two years in testing equipment," says Lori LeRoy, the company's co-founder. Global IC Trading Group is now mulling the purchase of a new machine, which would cost from \$40,000 to \$50,000, to examine the elements on a chip.

Intel, the world's largest chipmaker, has developed software to help customers identify the processor inside a machine and ensure that it's performing up to spec. Such steps have helped Intel rein in a problem that was more pervasive during the 1990s, says Intel spokesman Chuck Mulloy. The issue has "never gone away but it's not nearly as bad," Mulloy says.

PCX visually inspects all products but conducts acetone and other tests on about 10% of the roughly 50-to-100 products it receives daily. Two years ago, the company was able to fit all the counterfeit items it had detected on a single shelf that had space for thousands of variously sized components. The number of shelves has since expanded to three. Before long, Dimmler says, he'll need to devote further space for fakes.

King is a writer for Bloomberg BusinessWeek in San Francisco.