

JUNE 4, 2007

THE CORPORATION

By Eric Schine

Faking Out The Fakers

Faced with a tidal wave of counterfeit goods, companies are turning to secretive sci-fi technology. But crooks catch on fast.

Next time you fill up at the pump, there's a good chance you'll be injecting billions of nanoparticles into your tank. These marker molecules are in much of the gasoline at U.S. pumps, allowing gas companies to determine whether the fuel you're buying is the real stuff or some adulterated mix. If you think that's weird, a similar organic tracing compound may one day be coursing through your alimentary canal as you sip a scotch on the rocks.

After years of taking abuse from counterfeiters, companies and even nations are turning to advanced technologies to win back control of their brands and ward off accidents associated with fakes. The European Union and the U.S. are lurching toward creating anti-counterfeiting standards, but companies aren't waiting. They're applying the latest advances in molecular science and nanotechnology: injecting their products with nanotracers, dyeing them with invisible DNA markers, and engraving them with microscopic laser etchings. Stores, customs officials, or investigators will soon be able to see whether a product is real or fake by scanning it with a handheld reader and, in some cases, by matching it against an electronic database. In the most ambitious schemes, every glass bottle, plastic container, paper package, handbag, and pair of sneakers will have its own unique passport.

AstraZeneca PLC (AZN) is pushing this technology about as far as it can go. Outraged by the way counterfeiters have brazenly marketed fake drugs under its brand, the pharma giant has begun applying multiple layers of safeguards to 100 million packs of its ulcer medicine Nexium. Each blister pack of 30 pills contains a hidden molecular tag, a seal that fractures upon opening, and a hologram to reassure customers. All of this raises costs for would-be counterfeiters, although it hardly holds them at bay. But the next stage of the scheme, now in a pilot program, could raise the bar substantially if it were adopted in countries around the world. It will require pharmacies to scan advanced bar codes on each package describing exactly when and where the contents were produced.

When the code is scanned, the information embedded in it, including a random serial number, is instantly matched against a database. A match can only occur once. If any serial number pops up a second time, investigators are alerted. "We believe [the numbers] cannot be copied," says David Teale, AstraZeneca's director of product security. To further authenticate a batch of drugs, the investigators can check packages for hidden tags using special readers.

There's no shortage of companies seeking to supply such security systems to the likes of AstraZeneca, Xerox (XRX), 3M (MMM), Kodak (EK), NCR (NCR), and hundreds of smaller companies have all redoubled their marketing efforts in recent months for a simple reason: Counterfeiting has reached towering proportions. According to the International Chamber of Commerce, businesses lose about \$600 billion a year to counterfeiters, a figure that's on track to grow to \$1.2 trillion by 2009.

Fakes take a heavy toll on profits in the \$80 billion luxury-brand sector—the likes of Hermès and LVMH Moët Hennessy Louis Vuitton (LVMUY). But counterfeit wares can also injure and kill people. Cell phones have exploded because they contained counterfeit batteries. Automakers have discovered fake brake pads made of compressed grass trimmings. The Federal Aviation Administration currently estimates that 2% of the 26 million airplane parts installed each year are counterfeit—or 520,000 parts. "If you can make it, they can fake it," says Ed Dietrich of Reconnaissance International, an anti-counterfeiting consultancy.

Some security players, such as Eastman Kodak Co., opt to protect their anti-counterfeiting systems as trade secrets rather than patent them and create a paper trail that would-be pirates could scrutinize. Their reticence is understandable. Counterfeiters—well financed, and sometimes backed by organized crime—often can figure out how to fake the codes and holograms designed to outsmart them, and there's no reason to assume nanotech (the science of materials measured in billionths of a meter) is beyond their ken. "The half-life of a security system is a year or six months before someone is nipping at your heels," says Patrick K. Higgins, director of business development for JDS Uniphase Corp.'s (JDSU) Flex Products Group.

SKYROCKETING SALES

Although the authentication industry is still small, with estimated sales of just \$500 million, it's growing at a clip of 10% to 15% a year. For some startups, business is expanding much faster. Dallas-based Authentix Inc. uses technology acquired from Los Alamos National Laboratory to trace gasoline, pharmaceuticals, and beverages. The six-year-old privately held company's sales are increasing at a 35% pace, to \$25 million last year. Authentix works with both AstraZeneca and Royal Dutch Shell PLC (RDS), among others. Since late 2002, Authentix markers have helped weed out 20 wholesalers suspected of mixing their Shell-branded gas with a cheaper variety before passing it along to filling stations. In Brazil, where gas is routinely diluted with industrial solvents, the oil company ran a successful marketing campaign for its tagged gasoline under the banner "Shell DNA." The idea was to reassure consumers that Shell's fuel is constantly being checked for Authentix' markers.

Some of the most ingenious solutions are being deployed in the luxury market. Florence-based Solos bonds minuscule tags to fancy leather goods. Israel's Advanced Coding Systems Ltd. weaves a magnetic filament into high-end apparel. A Belgium-based European consortium called Naginels offers a laser engraving technique that etches code so tiny each letter or number measures just 3.5 microns in height. (Thirty of these letters would span the width of a human hair.)

Luxury companies rarely answer questions about how they're using such technology. But clearly, someone is buying. Signoptic Technologies, a French startup near Lyon, counts a dozen or so European luxury and pharma clients who have signed on to authenticate their products, and it has just opened an office in Boston. Signoptic has a

patent for a process that takes the equivalent of a fingerprint of each handbag, plastic bottle, or paper package as it rolls off the line, turns that into code, and stores it in a database retailers can access to verify a product.

Companies don't need to spend megabucks to get a modicum of protection. That's a good thing, because even your basic bottle of \$10 wine can be faked. Typically, a counterfeiter in China or Thailand will collect or fabricate Bordeaux bottles, refill them from tanks of cheap wine, and affix a false label. Since 2005, Geneva-based Algoril has signed up nearly two dozen Bordeaux producers. For a few cents per bottle, Algoril prints labels that give each one its own code, which customers can match against a database using their cell phones. Dominique Meneret, who just signed up with Algoril for his Domaine de Courteillac and Château de Brondeau wines, hasn't yet been faked, but "I prefer to take insurance for the future," he says.

A WIDE NET

Although still tiny, companies like Signoptic and Algoril have caught the attention of the French government and European bodies that are attempting to come up with a Continent-wide authenticating standard. "Our first priority is the health and safety of the consumer," says Pierre Delval, a former adviser to the French Ministry of Industry who now works for the 47-member Council of Europe. "We need to elevate counterfeiting to a criminal offense in Europe, but we can only do so if we have irrefutable proof of fakery. Technologies like Signoptic and Algoril help."

The problem with these database systems is that determined hackers could break into them and plant bogus codes corresponding to fake wines or any other product. That's why many large-scale consumer brands and manufacturers opt for a layered approach, wherein several technologies are combined in one product. When Germany's Beiersdorf started receiving complaints from consumers in Russia about its Nivea brand shampoo, the company investigated and found that some 30% of the bottles on store shelves in Russia were fake.

Beiersdorf turned to its subsidiary, Texas Scribos, which had invested \$25 million to develop a four-layer security system using techniques ranging from a simple hologram visible to the eye to encrypted microdata only readable with a digital decoder. By combining this technology with an intensive investigation, Beiersdorf was able to crack the counterfeiting ring within six months.

Schine is an Associate Editor at BusinessWeek