

Written testimony by

Steve DelBianco
Vice President for Public Policy
Association for Competitive Technology

Submitted to the
House Commerce Committee, Subcommittee on Commerce,
Trade, and Consumer Protection

"Product Counterfeiting: How Fakes Are Undermining U.S. Jobs,
Innovation, and Consumer Safety"

June 15, 2005

Mr. Chairman, Members of the Subcommittee, My name is Steve DelBianco, and I am Vice President for Public Policy for the Association for Competitive Technology (ACT). I would like to thank the Committee for holding this important hearing and I'm pleased to have the opportunity to testify on the impact of counterfeiting on small business.

ACT is an active part of the US Chamber of Commerce - Coalition Against Counterfeiting and Piracy (CACP), and I am here today as a CACP Member.

ACT is an international education and advocacy group for the technology industry. Focusing on the interests of small and mid-size entrepreneurial technology companies, ACT advocates for a "Healthy Tech Environment" that promotes innovation, competition and investment. ACT represents nearly 3000 IT and eCommerce businesses and professionals.

Today's other distinguished witnesses will better describe the devastating economic effects of counterfeiting on the industries that manufacture or create the name brand products we all know and respect. Without question, this half a trillion dollar drain on the global economy is felt by big business. But we cannot forget the effect on the retailer who makes the final sale to the customer, and the small business for whom even 5% in lost sales will turn the lights out for good.

For small retailers, whether online or on main street, counterfeiting can be devastating.

Counterfeits can ruin the most important relationship we have – customers who trust us. The small retailer depends on his wholesale suppliers to provide legitimate products, and is caught unaware when counterfeit goods make it onto his shelves.¹

If a counterfeit product fails, the retailer takes the blame. We have to deal with an angry customer who wants a replacement, or worse, a refund. If it's clearly counterfeit, our in-store managers have to figure how and where to return the product. Do we send it back

¹ Tim Trainer, president of the International AntiCounterfeiting Coalition, in <http://www.pcworld.com/news/article/0,aid,111319,pg,3,00.asp>

to the wholesaler? Do we need to contact the manufacturer? Most often, we just absorb the cost and work to regain the customer's trust.

All of this presupposes the customer decides to return the counterfeit. More often than not, the customer gets angry but doesn't bring the item in for replacement. Instead, the local store gets passed by the next time our former customer goes shopping.

Small retailers depend heavily on customer trust and respect, whether they're selling on main street or online, but in the growing world of e-commerce, establishing and maintaining that trust is even more challenging. Frankly, it says a lot about the growing consumer confidence in ecommerce that so many Americans will proffer their credit card for an online purchase from a supplier they've just selected from a list of search results. Yet, more consumers do it everyday, and they're overwhelmingly pleased with the quality, convenience, and value of e-commerce.

Small business is relying more on online distribution

Small manufacturers and specialty retailers are turning to e-commerce for their distribution and sales. According to Gartner Research, 30% of businesses with fewer than 20 employees and a Web presence now generate more than 25% of their sales online.²

E-commerce doesn't just benefit sellers of DVDs, software, iPods, and other technology-related goods. The benefits of e-commerce extend to industries that might not first come to mind. For example, a 2002 study confirmed that small farms value the Web as a business tool for reaching new customers, buying supplies, and streamlining their administrative processing.³

Small software companies can also take advantage of digital delivery, without the need to create and ship costly packaging or hefty paper manuals that go out of date with

² Mika Krammer, research director of the small and mid-size business group at Gartner

³ Ohmart, Jeri L., "Using E-commerce to Add Value to Small Farming Businesses in California," Study on Retail Farmers' Markets and Rural Development, Cornell University & Iowa State University, funded by the Fund for Rural America and the USDA, May 2002.

the next update. For any manufacturer, the ability to send a product to a customer the instant he wants it, with no warehousing or shipping costs, is the Holy Grail.

Online is the future, but online distribution attracts counterfeiters, too.

Online selling is attractive for large and small businesses, but it's also attractive to counterfeiters who want to exploit the instant reach and relative anonymity of the Internet. Counterfeiters have a long history of exploiting and undermining traditional distribution channels, whether by infiltrating the supply chain or circumventing it entirely through flea markets and street vendors. But now they're learning that online selling offers some advantages over selling from physical locations.

In the physical world, a store can't pretend to be something it isn't. Unless you are attempting to pull-off '*The Sting*', one doesn't construct an artificial storefront to lure people into purchasing counterfeit goods. Online stores, on the other hand, are relatively simple to create and operate. And the Internet lets a website in Singapore be instantly visible to the entire world.

The fight against counterfeit goods has to be taken beyond the retail level. Industry and law enforcement efforts have to focus on the source -- producers, wholesalers, and distributors of counterfeit goods. And the primary source is, not surprisingly, China.

The Hangzhou-based *Alibaba* website (www.alibaba.com) is a virtual market where major players in the underground counterfeiting network connect and trade. While some authentic goods are traded on Alibaba, counterfeiters are in evidence all over this website, in both English and Chinese language renditions.

On Alibaba, many sellers are explicitly seeking worldwide distributors for their counterfeit goods, including software, prescription drugs, golf clubs, apparel, and even batteries. Below is an actual Alibaba screen offering large lots of counterfeit Duracell batteries, claiming they were produced using "good materials" and promising "value for money".



Counterfeit exchanges like Alibaba will undoubtedly harm China's consumers and impair the future of legitimate e-Commerce there. But Alibaba can also drag other economies down with it, by injecting wholesale quantities of counterfeit goods into the worldwide supply chain.

While Alibaba has created a growing marketplace for counterfeit physical goods, there is another side to counterfeiting that is especially destructive to ACT's small software developers: *digital* distribution sites that claim to be legitimate, but aren't.

Software piracy and counterfeiting: double jeopardy

It's important to note that there is a real distinction between *piracy* and *counterfeiting* when it comes to software. We are all aware that strictly-digital pirated copies of software are downloaded every day from file-sharing services like Grokster and eDonkey. When a user grabs a free digital download of Microsoft Word from these file-sharing sites, he knows without question that he's stealing a pirated copy of the software. There is not the least pretense of legitimacy from the person giving the copy, from the file-sharing service, or in the mind of the person downloading the copy.

Contrast that pure form of digital piracy with counterfeit software copies that come in tangible form, complete with packaging. On street corners and websites worldwide, you can buy CD-ROM copies of leading software from Microsoft, RedHat, Symantec, Norton, Adobe, and Corel.

For example, SoftwareNow draws people to its website through emails claiming “*Prices slashed to the bone on original U.S. PC software!*” SoftwareNow’s slick website shows pictures of packaged software available at a fraction of retail prices. On their site, here’s how SoftwareNow answers the wary consumer wondering how they can sell so low:



How can you sell this software as OEM ? It seems too good to be true - is there a catch?

There is no catch - the software versions that we sell are OEM (Original Equipment Manufacturer) which means you will receive the installation CDs only (they do not come in their original retail packing and do not include the manual). We do guarantee that all programs are the 100% full working retail versions - no demos or academic versions! When you order, you will receive all materials required for a complete installation - or your money back! Why pay hundreds of dollars more when you can get exactly the same but OEM-CD? You don't have to pay that much for the fancy box and manuals.

Although SoftwareNow claims they’re selling OEM versions of software from manufacturers like Microsoft, you cannot buy so-called OEM software without buying the computer itself from the OEM. But not many consumers are aware of that, so many are taken-in by the ruse.

Counterfeit Software is a security risk

Consumers who are unfortunately duped into buying counterfeit software may never discover that they’re running counterfeit code. After all, digital copies are perfect copies, so the software looks and performs like the real thing. But that only helps lure users into a false sense of security when it comes to getting notifications and updates to respond to new cybersecurity threats.

Returning to the SoftwareNow example, there’s a dangerous disclaimer buried on the website, warning buyers, “*Note, that you will not be able to register the software with*

the manufacturer and get their support, but we will do our best to support you any way possible.”

Not many consumers would be as alarmed as they should be by this “disclaimer”. Those who purchase and install the counterfeit software could go for months without knowing they are missing critical notices and software updates to prevent security vulnerabilities. This compromises their own security against viruses, spyware, and identity theft.

Moreover, their unsecured PC can serve as a platform for other bad actors to exploit for spam relays, virus proliferation, and denial of service attacks. Counterfeit software can contain Trojan Horses or open “back doors” that let criminals into a user’s computer.

Taken together, piracy and counterfeiting are costing the software industry \$30 billion each year, and IDC estimates that 1 in every 3 PCs worldwide contains some pirated or counterfeit software. In 2002, seizures of pirated Microsoft products alone exceeded \$1.7 billion.⁴ And these costs don’t include the wider costs to businesses and consumers of vulnerable PC software that’s not registered with the manufacturer and not getting timely notices and security updates.

Government and Industry are fighting back

A Justice Department study in October 2004 describes several examples of how industry and the U.S. Government are battling software counterfeiters. In 2003, a Virginia man was sentenced to five years in prison and ordered to pay \$1.7 million in restitution for selling more than \$7 million in counterfeit software over the Internet. In a 2004 prosecution, a Ukrainian man was charged with illegally distributing millions of dollars of unauthorized copies of software from Microsoft, Adobe, Autodesk, Borland, and Macromedia. And in September 2004, DOJ’s “Operation Digital Marauder” seized over \$56 million in counterfeit Microsoft software, and charged 11 people with manufacturing counterfeit software and counterfeit packaging.

⁴ Statement of Richard C. LaMagna (Microsoft Corporation) before the House Subcommittee on Courts, the Internet, and Intellectual Property, Oversight Hearing on International Copyright Piracy: Links to Organized Crime and Terrorism, (March 13, 2003)

The next generation of e-commerce...and of counterfeiting

The next generation of e-commerce will see more goods delivered in entirely digital form—with no packaging at all. Digital delivery of music, software, books, art, and movies will all depend on trust relationships that are created and maintained by technology.

Digital content will be streamed via broadband, but the creators will need a way to know that you are a bona fide buyer, and buyers will need to assure they are acquiring a legal copy from a legitimate vendor. This future world will turn President Regan's adage "*trust, but verify.*" on its ear – the future of digital goods will "*verify, to create trust*".

We all know what the breakthrough success of Apple's iTunes service has done to legitimize digital music downloads. But what you might not realize is that iTunes relies on digital seals and certificates, the electronic means of authenticating that you are who you say you are.

To make this possible, e-commerce infrastructure leaders like VeriSign, eBay, and Microsoft are developing certification technologies and programs to authenticate the legitimate identity behind emails, websites, and the products themselves. Automated authentications occur quickly and without human intervention, so shoppers are notified only when there's a question about certifications claimed on a store website. If a consumer has to telephone the manufacturer or check lists of authorized dealers, he loses some of the convenience that makes e-commerce attractive in the first place.

Digital seals and certificate services are used by e-commerce sites to prove identity and show they're using secure communications. VeriSign's Secured Seal, for instance, shows that a website has been approved by VeriSign to protect credit card and other confidential information with SSL encryption. Similar technologies help to assure a customer that his bank website really is *his* bank.

New technology behind RFID (Radio Frequency Identification) tags and the Electronic Product Codes network will help stop fakes from penetrating supply chains.

Drug shipments, for instance, can be automatically scanned and authenticated as they travel from manufacturer to pharmacy. The pedigree and location of drug shipments will be accessible to all parties, preventing copies from being introduced into the supply chain.

However, these certification technologies could themselves be subject to elaborate counterfeit schemes. Criminal email phishing schemes are luring users to a website that has the marks and logos of legitimate security providers, and some present a 'certificate' that the user can accept or refuse. Unfortunately, many users don't read the certificate closely, and are duped into believing it's real. This gives small software firms an abiding fear that a criminal could fake the security certificates for a sales page, and sell digital downloads of software to people who really are trying to buy a genuine product.

For the digital future to fulfill its promise, customers will need to trust the person at the other end of the wire. And if you can't shake their hand, you'll need digital certificates and authentication methods to give you the same sense of trust. When—*not if*—criminals begin to forge security keys, hash codes and security certificates, industry will need to work even more closely with law enforcement to investigate and aggressively prosecute counterfeiters.

Conclusion

To summarize, we see three critical points for policymakers to consider when confronting the problems posed by counterfeit goods:

1. Counterfeiting is a huge drain on the economy - it affects everyone from manufacturer to final retailer, destroying the most valuable commodity we have: the trust of our customers.
2. Illegitimate exchanges like Alibaba are moving counterfeit goods from the streets to websites. The U.S. Government needs to exert pressure on foreign nations to shut this activity down.

3. The next war in counterfeiting will be waged not with physical boxes but with digital seals and certificates. Goods that can be delivered digitally will depend on digital signatures, physical goods will be bought and sold from stores using authentication to create and maintain trust relationships with customers.

The technology industry is constantly driven by market forces to help its business partners solve problems quickly and cost-effectively. We look forward to working with Congress and the Administration to encourage aggressive enforcement against counterfeiters, and convincing our trading partners to do the same.

CACP Membership List

As of June 22, 2005

Associations

1. Advanced Medical Technology Association (ADVAMED)
2. AeA, Advancing the Business of Technology (AeA)
3. Aerospace Industries Association (AIA)
4. Alliance of Automobile Manufacturers (AAM)
5. American Apparel & Footwear Association (AAFA)
6. American Association of Exporters and Importers (AAEI)
7. American Council of Independent Laboratories (ACIL)
8. American Intellectual Property Lawyers Association (AIPLA)
9. American Society of Association Executives (ASAE)
10. Association for Competitive Technology (ACT)
11. Association of Equipment Manufacturers (AEM)
12. Automotive Aftermarket Industry Association (AAIA)
13. Center for Health Transformation (CHT)
14. The Cosmetic, Toiletry and Fragrance Association (CTFA)
15. Consumer Electronics Association (CEA)
16. Electronic Industries Alliance (EIA)
17. Entertainment Software Association (ESA)
18. Food Marketing Institute (FMI)
19. Gas Appliance Manufacturers Association (GAMA)
20. Global Business Leaders Alliance Against Counterfeiting (GBLAAC)
21. Grocery Manufacturers of America (GMA)
22. International Anti-counterfeiting Coalition (IACC)
23. International Federation of Phonographic Industries (IFPI)
24. Intellectual Property Owners Association (IPO)
25. International Communications Industries Association (ICIA)
26. International Trademark Association (INTA)
27. Motion Picture Association of American (MPAA)
28. Motor & Equipment Manufacturers Association (MEMA)
29. Motorcycle Industry Council (MIC)
30. National Association of Manufacturers (NAM)
31. National Electrical Manufacturers Association (NEMA)
32. National Marine Manufacturers Association (NMMA)
33. Outdoor Power Equipment Institute (OPEI)
34. Pharmaceutical Research and Manufacturers of America (PhRMA)
35. Recording Industry Association of America (RIAA)
36. Specialty Equipment Market Association (SEMA)
37. Toy Industry Association (TIA)
38. U.S. Chamber of Commerce (USCC)
39. U.S. Council for International Business (USCIB)
40. Vision Council of America (VCA)

CACP Membership List

As of June 22, 2005

Corporations

1. Altria Corporate Services, Inc.
2. Altria Group, Inc.
3. American Standard Inc.
4. Amgen Inc.
5. AOL Time-Warner
6. Aspen Systems Corporation
7. Baker & McKenzie
8. BellSouth Corporation
9. British American Tobacco
10. C&M International, LTD
11. Dayco Products, LLC
12. deKieffer & Horgan
13. DuPont Security & Solution
14. Eastman Kodak Company
15. Gallup
16. Gillette
17. Intel Corporation
18. Jones Day
19. Kent & O'Connor, Incorporated
20. National Broadcasting Corporation (NBC)
21. News Corporation
22. Oakley
23. Pernod Ricard USA
24. Pfizer
25. Robert Branand International
26. Stanwich Group LLC.
27. The Fairfax Group
28. Tiffany & Co.
29. Torys, LLP
30. Transpro, INC
31. Underwriters Laboratories, Incorporated
32. USA For Innovation
33. Verizon
34. Xerox Corporation