Deploying Technology to Fight Counterfeiting

Adrian P Burden is the President, Europe at Bilcare Technologies (formally Singular ID)

Introduction

Counterfeiting and piracy have become high technology industries in themselves. The sophistication used to copy products often means that fakes are ostensibly identical to the originals. This presents a huge problem for all of the stakeholders; from the brand owner, through the supply chain to the end consumer.

More importantly the problem cuts across every sector causing specific issues in specific markets. Copied luxury handbags may not present a health risk to the end consumer, but the revenue generated from sales often promotes illegal child labour in third world countries[1]. Fake apparel and sportswear may last just as long as the real thing, but almost certainly finances terrorist activity somewhere in the world[2]. Then there are products that really do cause health and safety issues – from bogus car parts that can contribute to road accidents, fake wines and spirits that contain harmful ingredients, to counterfeit medicines that either provide no medication at all or give the wrong medication[3].

When it comes to piracy; the copying of music, software, and other copyrighted media, the problem is compounded by the ethereal nature of the digital product[4]. Media can be replicated with various levels of quality, but in many cases up to the level of the original with relative ease. This presents its own technological challenges to overcome, as digital media can be supplied without packaging and without importation through a customs agency.

Despite the fact that public awareness of the problem is growing, few consumers or indeed employees of brands are fully conversant with the extent of the problem[5]. There are several contributory factors to this; the reluctance of many brands to discuss the problem for fear of losing trust and reputation within their consumer base, the difficulty in measuring the extent of counterfeits as they travel alongside legitimate products within the supply chain, and the fact that consumers are barraged daily with news and advertisements, and so any message about counterfeits barely peaks above the background noise. This lack of awareness can also make the effective implementation of a brand security technology more difficult, because some form of education or marketing is usually required to ensure that the technology is recognized and used properly.

A diverse problem

There are numerous published statistics about the extent of counterfeiting, and there are many organizations around the world attempting to combat the crime[6]. But it is always instructive to look at these facts and reflect on how technology might be deployed to have an effective impact on the problem.

Firstly, headline figures quoted by reputable sources such as Interpol, the World Customs Organization (WCO) and the International Chamber of Commerce (ICC) put the annual value of counterfeit goods as being equivalent to about 5-7% of world trade or (US$500 to US$650 billion)[7],[8]. This is a sizeable figure (more than the annual revenue of world's largest retailer Wal-Mart, which for the financial year ending January 2008 had sales revenues of just under US$375 billion)[9]. As such, it would seem reasonable to make investments in sophisticated technology to reduce the problem. The difficulty many brand owners face is quantifying the losses so that they can gauge the likely return on such an investment.

Counterfeiting is also a rapidly growing industry, and has increased unabated for many years[10],[11]. The recent credit crunch and economic downturn may have adversely affected legitimate manufacturers, but there is evidence that this has fuelled trade in fake products. Partly because low cost fakes are more appealing to the cash-strapped consumer[12] and also because in this industry cash flow is governed more by criminal activity than lines of credit from high street banks[13].

In the fashion industry, the impact of the problem is difficult to gauge because the argument goes that people who buy fakes would not usually buy the much-more-expensive genuine products. There is bound to be some element of truth to this, but ultimately, the lower cost fakes are being sold in lieu of mainstream products from lower-end brands, and so revenue is still being made illegitimately whilst taxes and duties are almost certainly being evaded[14]. Fashion and luxury is also a very broad market sector, with products including clothing, suits, shoes, sportswear, handbags, watches, perfumes, cosmetics and jewellery for example. The manufacturing and distribution practices for these different product lines are also diverse and so universally protecting a brand, either with improved business practices or through the use of technology, can be a major challenge.

Looking at another very different sector by way of example, the Motoring Equipment Manufacturers Association (MEMA) in the US estimates that counterfeiting costs the global automotive parts industry US$12 billion per annum with US manufacturers losing about US$3bn in annual sales[15]. The problem has lurked in this industry for years and has not yet been satisfactorily addressed[16]. Much of the problem stems from the fact that cars require replacement parts during their life and the fitting of these is often trusted to workshops and mechanics, sourcing goods from a complex international supply chain. Moreover, parts range in shape, size and operating requirements which can present challenges when deploying a technological brand protection solution; particularly if it is to protect a part directly rather than the packaging.

Perhaps the most alarming market sector in which counterfeit goods are rampant is that of pharmaceutical and medical products[17]; to the extent that respected academic journals have also reported the problem[18],[19]. The World Health Organization (WHO) International Medical Products Anti-Counterfeiting Taskforce (IMPACT) is cautious in stating the size of the problem[20], although in the past the WHO has reported estimates of as much as US$35 billion of counterfeit medicines being sold globally per year. The medical supply chain is complicated; local legislation in different territories requires repackaging and relabeling, and in recent years the sale of medicines over the internet has rapidly increased. All of these problems present serious difficulties in preventing fake products entering a market, and unfortunately it is the developing countries with malaria, AIDS, and relatively poor healthcare in general that suffer the most from the scourge.

More information, resources and news about counterfeiting in these and other sectors is available at the BASCAP website (www.bascap.com) and at the No to Fakes website (www.notofakes.com).

Deploying technology

Brand owners and manufacturers have often resorted to technology involving marking their product packaging to try to thwart the menace of counterfeiting. Probably the most common and most overt technique is the use of a hologram, once a high-technology solution that was deemed difficult to replicate. Today, holograms and similar optical-effect labels can be reproduced passably and with relative ease, and counterfeit products have even sported holograms where the original does not!

This fact provides an insight into a major issue relating to counterfeit prevention. The consumer is difficult to educate, and highly unlikely to tell a genuine hologram from a crude imitation. Not only that, but to a consumer, holograms are synonymous with security so counterfeiters can leverage this understanding to sell more product.

Engineering components and spare parts have often relied on serialization to provide some level of counterfeit protection. This is particularly so in the aviation industry; the argument here being that individually numbered items will have a paper-trail of traceability demonstrating the pedigree of the part. However, copying and altering numbers is a relatively straightforward task, even when they have been shot-peened or laser marked using capital-intensive equipment. This results in confusion, as the original and fake with the same serial number cannot easily be distinguished and depending on which one gets checked first, a fake may pass into use ahead of the genuine one.

Radio-frequency identification (RFID) is the latest way to serialize items; making use of a silicon chip to store the unique number and in some cases additional information. However, RFID is not without its problems; it is still relatively expensive compared to simple numbers and barcodes, it comes in a variety of formats with very different levels of security, clones can be made to broadcast the same number, and in some instances the metallic or liquid environment makes RFID unreliable. However, RFID is here to stay as a logistics tool, and certainly helps raise the hurdle of counterfeiting. Used alongside other security technologies, it can be a very powerful tool.

When a brand owner considers a technology for brand protection, many questions need to be addressed, as illustrated in Exhibit 1. The strategy needs to be considered throughout the supply chain and the product lifecycle. A risk analysis needs to be conducted on how and when products should be authenticated, but it also needs to address the necessary action if an authentication fails. At the end of a product's life, there must be no danger that the security feature can be unscrupulously reused on an illegitimate product.

In addition, the brand owner needs to know if a solution should be used in isolation or as part of a layered security system. Money and passports, for example, have long been issued with multiple layers of security; because if one layer is compromised, there is a strong likelihood that others will remain intact. There are also different solutions for different types of authentication: the look and feel of the banknote is often enough for a consumer to be confident that the money is genuine; the shopkeeper may resort to ultraviolet light to verify a watermark; whereas a bank will use other machine readable technology to provide yet higher levels of confidence in the process. The same approach should be used to protect products.

The next step is to consider the means of authentication at each level; particularly if human observation is to be relied upon (usually less expensive in terms of equipment out in the field being unnecessary, but certainly less secure as consumers and officials alike are easily duped). Where a reader is to be deployed, whether it is a simple "filter" to change the appearance of a genuine label or a more sophisticated scanner to read a tag, consideration needs to be given to the cost and the location. Verification at the actual point of sale is usually the most powerful approach, but the vendor needs to be incentivized and the consumer needs to expect it as part of the service. Exhibit 2 highlights some of the considerations and drivers that exist along a supply chain.

As such, one of the principal hidden costs in the use of any technology deployed to thwart counterfeiting is in educating the consumer to know what to expect and how to discern genuine products from fake. Brand owners often overlook this fact, and sophisticated technology may provide a disappointing return on investment if an education plan has not been rolled-out in parallel.

The specific requirements of different sectors also challenge how a technology might be successfully deployed. For example, fashion items are often limited editions or bespoke products made using high-quality materials in novel and distinctive designs. The product range is often diverse and delivered in a high mix of low volume. The anti-counterfeiting technology must not impact on the aesthetic design of the item, whilst still providing a means of security that can ideally be authenticated by the consumer. Genuine fashion items often become collectables, and although the brand owner may not wish to promote resale, an authentication technology that can last the lifetime of an item brings value to the end-user and ultimately respect for the brand. Analyzing these different drivers helps to establish where value is likely to be perceived in a deployed system. Ideally, value needs to be derived at each point in the supply chain, as highlighted in Exhibit 3.

Spare parts are usually carefully engineered to work in aggressive environments. For example, replaceable items like gaskets, plugs, filters and pumps might need to operate at elevated temperatures, in high humidity or in oily conditions. This is not just the case for cars, but also for public transport, aircraft, industrial applications such as power stations, in refrigerators, etc. Brand owners often make most of their revenue on after-sales servicing, and so there is a need to protect the supply chain to safeguard business as well as the reputation of the brand. As such, brand owners will realize that a suitable technology often needs customization to work favourably with the nuances of a particular product.

For pharmaceuticals, the primary packaging (such as the blister pack) is the most useful part to protect, because outer cartons are often replaced in different markets to cater for differences in language and label legislation. Some technologies even exist to directly mark the tablet, but there are limitations as to the ease of verifying such markings in the supply chain. However, another consideration is the sheer volumes of products that are produced each year. A suitable anti-counterfeiting technology needs to be cost-effective for very low-cost but high-volume items. Protecting the high-end medicines is not enough, because even low-cost generic painkillers such as Aspirin are found to be lucrative products for counterfeiters.

Materials solutions and an integrated approach

A powerful approach to brand protection is through the use of materials and chemicals to provide the equivalent of a "fingerprint" or "DNA" for a product. A number of techniques have been researched and developed to achieve this, including the use of the unique fibre arrangements in paper[21] and packaging[22] and the use of composite materials[23]. As a result, these technologies can be deployed in the form of a label, tag or by embedding the identifier in the product itself. Often these technologies work synergistically with serial numbers, barcodes and RFID chips, because the ease of reading a number helps make the authentication step quicker. This is analogous to checking a passport photograph in a database by first using the passport number as an index to find the correct entry quickly.

The power of this approach is that each product then has its own unique identifier, often constructed from very small and complex features, such that they are prohibitively difficult to reproduce. Ideally, the arrangement of the features is left entirely to nature and not directed by a predefined pattern, mask or design. If the features being measured are invisible (rather than being optical features), then the standard tools for photocopying or lithographically reproducing the "fingerprint" do not apply, and this raises the bar to duplication yet further. As the size scale drops in to the micrometer and nanometer regime, so the security rises yet further.

Solutions such as these are often fully integrated with a remote database so that the original "fingerprint" can be verified against one read later in the supply chain. This has become possible because telecommunications links are now widely available in the form of the internet, wireless connectivity and mobile phone systems. This means a remote database can be contacted quickly and inexpensively so that not only the authenticity of a product can be checked, but additional information such as expiry date can also be disseminated. This brings value beyond anti-counterfeiting, because if embraced by the supply chain, it also provides track and trace information that can improve efficiency and lower costs in other areas.

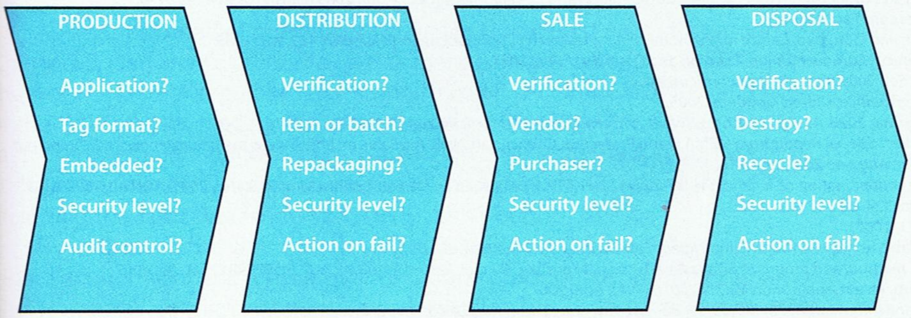
Exhibit 4 illustrates the concept, showing the components of this kind of high-end brand security technology. The product is protected with a tag, a scanner authenticates the tag and takes away any subjectivity of the authentication process, and a database not only provides authentication information, but also a fully updated audit trail capable of disseminating information in real time.

Outlook and conclusions

Deploying ever more sophisticated anti-counterfeiting technology is likely to be the only near-term solution to reducing the prevalence of fake products. Moreover, these solutions will need to be fully integrated to enhance security as well as bring value to each stakeholder in the supply chain. Because counterfeiting affects virtually all product sectors, and different products have specific forms, modes of use and customer expectations, the technology to provide the brand security is likely to require some level of customization to be effective.

The author (adrian.burden@singular-id.com) acknowledges his colleagues at Bilcare Technologies for input and discussion during the writing of this article; particularly Peter Moran, Praful Naik, Raman Nanda, and Jessica Williams.

EXHIBIT 1



PRODUCTION
Application?
Tag format?
Embedded?
Security level?
Audit control?

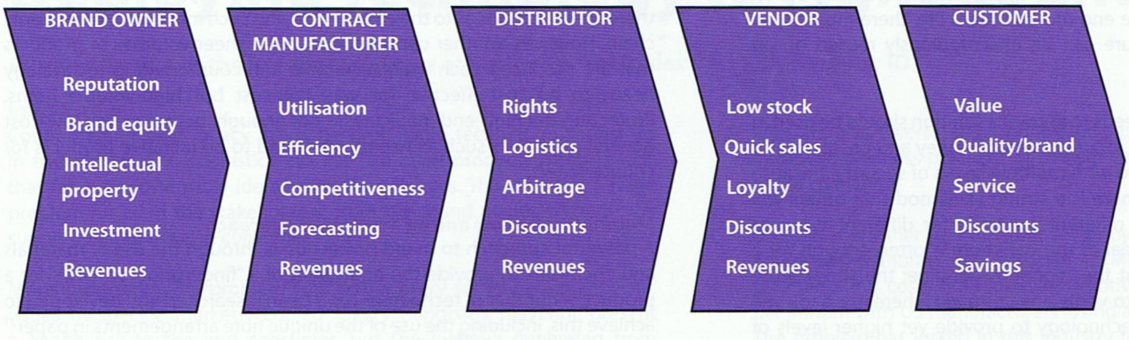
DISTRIBUTION
Verification?
Item or batch?
Repackaging?
Security level?
Action on fail?

SALE
Verification?
Vendor?
Purchaser?
Security level?
Action on fail?

DISPOSAL
Verification?
Destroy?
Recycle?
Security level?
Action on fail?

Some of the questions relating to how a deployed brand security technology should be used and moderated throughout the product lifecycle.

EXHIBIT 2



BRAND OWNER
Reputation
Brand equity
Intellectual property
Investment
Revenues

CONTRACT MANUFACTURER
Utilisation
Efficiency
Competitiveness
Forecasting
Revenues

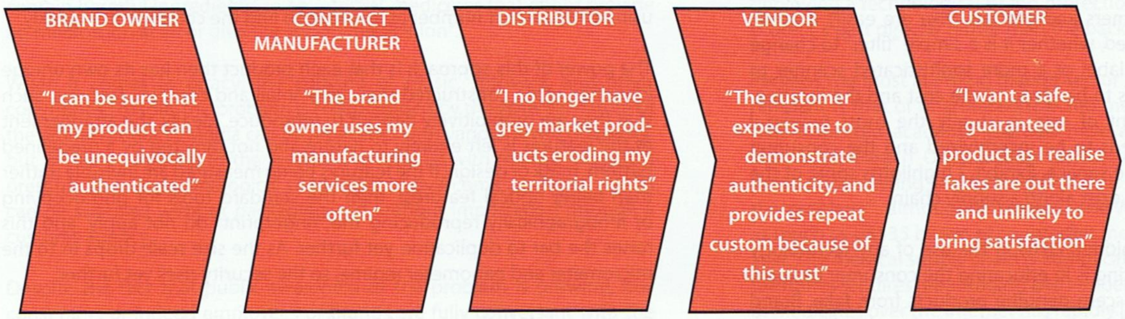
DISTRIBUTOR
Rights
Logistics
Arbitrage
Discounts
Revenues

VENDOR
Low stock
Quick sales
Loyalty
Discounts
Revenues

CUSTOMER
Value
Quality/brand
Service
Discounts
Savings

Some of the drivers and considerations of the parties across the supply chain. Unfortunately, many are in conflict with the notion of full-priced genuine products being preferential to lower cost fakes, and few encourage an authentication step.

EXHIBIT 3



BRAND OWNER
"I can be sure that my product can be unequivocally authenticated"

CONTRACT MANUFACTURER
"The brand owner uses my manufacturing services more often"

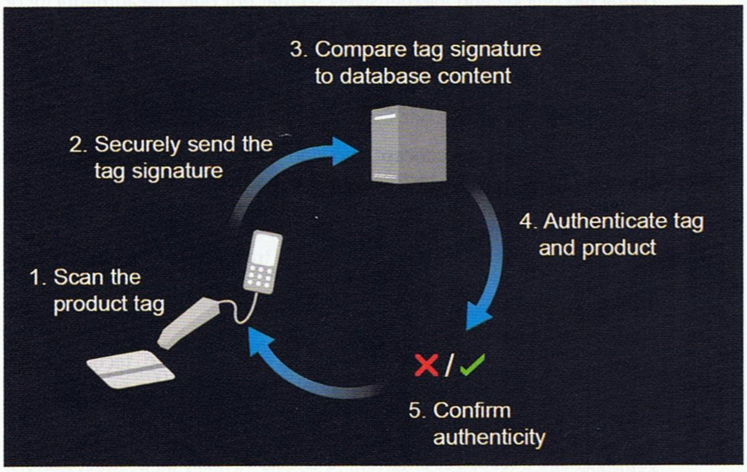
DISTRIBUTOR
"I no longer have grey market products eroding my territorial rights"

VENDOR
"The customer expects me to demonstrate authenticity, and provides repeat custom because of this trust"

CUSTOMER
"I want a safe, guaranteed product as I realise fakes are out there and unlikely to bring satisfaction"

Identifying the value an anti-counterfeiting solution brings to each stakeholder is paramount. Often there is a need to offer more value than simply 'anti-counterfeiting', such as supply chain management, warranty management or preventing product diversion.

EXHIBIT 4


3. Compare tag signature to database content
2. Securely send the tag signature
4. Authenticate tag and product
1. Scan the product tag
✗ / ✓
5. Confirm authenticity

Making use of a scanner and remote database to authenticate a materials-based "fingerprint" and prevent the counterfeiting of products.

1. "The Fake Trade: wanted for stealing childhoods" by D Thomas, published in Harper's Bazaar, Singapore, Mar 2007 (pp 210-213), and Harper's Bazaar on-going "Fakes are Never in Fashion" campaign at www.fakesareneverinfashion.com.
2. "The Fake Football Shirt Sting", BBC News, 3 Mar 2006, http://news.bbc.co.uk/1/hi/business/4768454.stm.
3. "Knockoff: The Deadly Trade in Counterfeit Goods", by T Phillips, published by Kogan Page Ltd, 2005 (ISBN 07494 4379 0).
4. "The Keys to Ending Music Piracy", by J Black, Business Week, 27 Jan 2003.
5. "Counterfeiting Culture", New Statesman, 22 May 2006.
6. "Fakes", Business Week, 7 Feb 2005.
7. International Chamber of Commerce (www.iccwb.org), through their initiative called Business Action to Stop Counterfeiting and Piracy (BASCAP) 2009.
8. "The Economic Impact of Counterfeiting and Piracy", published by the Organisation for Economic Co-operation and Development (OECD), Jun 2008 (ISBN 9789 2640 4551 4).
9. "Corporate Fact Sheet", Wal-Mart. Available at http://walmartstores.com/FactsNews/
10. "Counterfeit-Product Trade, A Growth Industry", by GM Grossman and C Shapiro, Centre for Economic Policy Research (CEPR), Discussion Paper No. 103, Apr 1986.
11. "Report on Community Customs Activities on Counterfeit and Piracy", European Union, Taxation and Customs Union, 2007.
12. "Counterfeit Bags Popular in Down Economy", Eyewitness News, Feb 2009 (http://tinyurl.com/cushsy).
13. "National Intellectual Property (IP) Enforcement Report", The Patent Office, United Kingdom, 2005.
14. "The High Price of Counterfeit Goods", by A Fox, Gotham Gazette, Mar 2008. Available at: http://www.gothamgazette.com/article/crime/20080331/4/2476.
15. "Intellectual Property: Protecting Valuable Assets in a Global Market", Special Report from MEMA Brand Protection Council, Jan 2008. Available at: http://www.mema.org/enews/pdf/brand.pdf.
16. "What's at Stake when it's Fake", by L Toussant, Aftermarket Insider, Aug-Sep 2003, pp12-15.
17. "Dangerous Doses – A true story of cops, counterfeiters, and the contamination of America's drug supply", by K Eban, published by Harcourt Books, United States, 2005, ISBN 0 15 603085 3.
18. "Murder by fake drugs", P Newton et al. British Medical Journal vol 324, pp 800-801, 2002.
19. "Bitter Pills", A Jack, British Medical Journal, vol 335, pp 1120-1121, 2007.
20. "Counterfeit Drugs Kill!", WHO IMPACT brochure, May 2008, available at http://www.who.int/impact/FinalBrochureWHA2008a.pdf.
21. "Authenticity determination system, authenticity determination method, and program", S Tadashi, K Tetsuya, I Kensuke, O Kenji, Patent Application JP2007279812 (A), Oct 2007.
22. "Authenticity verification of articles using a databases", R Cowburn, Patent Application MX2007001857 (A), April 2007.
23. "A method of identifying an object and a tag carrying identification information", PM Moran, AP Burden, Patent Application US2005/0017082, Jan 2005.