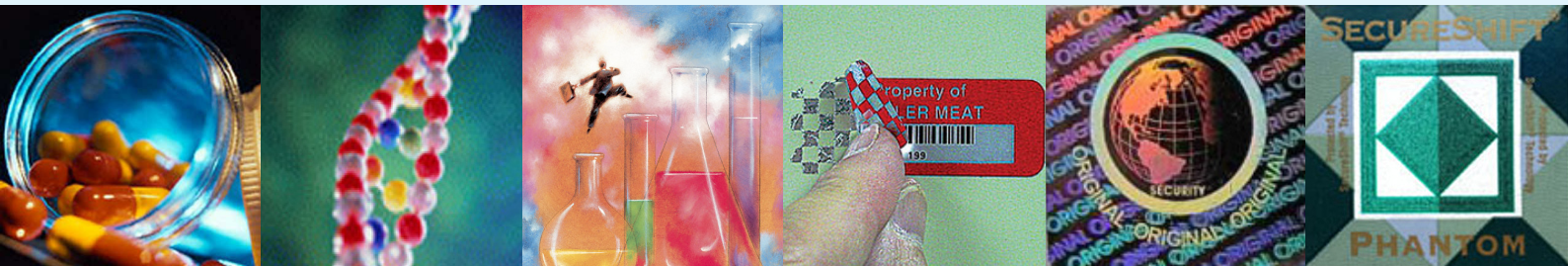




Confederation of Indian Industry

Technology Solutions

A Primer for Combating Counterfeiting & Piracy



"All information contained in this booklet has been obtained from sources believed to be accurate by CII. While reasonable care has been taken in its preparation, CII makes no representation, express or implied, as to the accuracy of the information. All information should be considered solely as statements of opinion"

Copyright: Confederation of Indian Industry – December 2008

Technology Solutions
A Primer for Combating Counterfeiting & Piracy

Acknowledgements

This manual was compiled by CII on the basis of numerous interviews with industry leaders, security specialists, and various providers of anti-counterfeiting technologies. Additionally, there has been significant review of information in the public domain, most notably from internet sources that have been cited in the text. We are immensely grateful to the many individuals who have offered information and opinion during the process of assembling this manual. We would particularly like to thank Prof. Avi Chaudhuri, PhD, of McGill University, Montreal, Canada, for his invaluable services in compiling this manual.

Comments and requests for additional copies (including electronic versions) of this document may be sent to:

Anjan Das
Senior Director
Confederation of Indian Industry
249-F Udyog Vihar
Sector 18, Phase IV
Gurgaon 122 015, INDIA
Email: anjan.das@ciionline.org

Contents

	Foreword	1
A.	Introduction	3
B.	Brand Protection — Options and Arguments	4
	1) The <i>laissez-faire</i> attitude	4
	2) The proactive approach	6
C.	Choosing the Right Technology — The Five Golden Qualities	11
	1. Consumer empowerment	12
	2. Cost and value	12
	3. Forensics and interdiction	13
	4. Simplicity and adaptability	14
	5. Value-added features	15
D.	Currently Available Anti-Counterfeiting Technologies	17
	1. Passive technologies	17
	a) Holograms and security seals	17
	b) Overt and hidden imaging	18
	c) Package modification	20
	2. Active technologies	20
	a) Electromagnetic taggants (RFID)	20
	b) Forensic taggants	22
	3. Mass encoding	24
	a) Barcode application	24
	b) Digital mass serialization (DMS)	26
	c) Digital mass encryption (DME)	28
E.	Technology Comparisons	31
F.	Choosing the Right Technology — Recommendations for Indian Industry	36
G.	Appendix — Selective List of Technology Companies	40

Foreword

It is now accepted by all stakeholders — from brand owners, to consumer groups, to policy makers — that brand counterfeiting and piracy represents a substantial problem that needs to be immediately tackled through a concerted effort by all parties. It was therefore a pleasure for me to read and review the new manual that CII has created titled *“Technology Solutions: A Primer for Combating Counterfeiting and Piracy”*.

Although all groups recognize the immense economic and social problem created by counterfeit products, the past approach by many organizations studying this issue has been to merely describe the counterfeiting problem and propagate the statement that “more should be done”. What is refreshing about this new manual is that CII is leading the way by showing brand owners just what it is they can do, and more importantly, why they should take a proactive role in protecting their brands and consumers.

This CII manual will be of immense value in terms of pedagogy and advocacy, which was clearly the goal in developing the document. As the largest and most influential industrial trade organization, CII is in the best position to present an objective evaluation of anti-counterfeiting technologies that are currently available in the marketplace. It has done this in a manner that is extremely readable to both tech-savvy corporate managers and the more strategically-minded senior management. The clear-cut opinions provided by CII also help provide an objective appraisal of available anti-counterfeiting solutions. In effect, CII has done the due diligence for Indian industry, and for this they are to be highly commended.

I believe that this manual will now become the default reference document in this field. Indian corporate executives should read this manual carefully, understand it, discuss it, and use the information to make a sound strategic decision on how to proceed. This is an opportune time for Indian companies to implement anti-counterfeiting solutions. This manual, for the first time, shows the road forward to those who are still undecided on the optimal solution.

Again, I offer my congratulations and appreciation to CII for this immensely valuable body of work. This will stand out as an important contribution to Indian industry.

Yours sincerely,



Malvinder Mohan Singh

Chairman, CII National Committee of IP Owners &
CEO and Managing Director
Ranbaxy Laboratories Ltd.

A. Introduction

The incredible growth and globalization of the Indian economy has been accompanied by major advances in the visibility of power brands. The escalating economic pyramid and resulting expansion of the middle class has produced unparalleled growth in virtually every product sector. The accompanying growth of grey-market products, however, has tainted the image of many Indian brands and reduced consumer confidence in their authenticity, whose establishment in the marketplace required significant and sustained investment on the part of their owners. As a result, opportunistic counterfeiting and piracy have become significant problems in India and now pose striking threats in terms of brand equity, safety, and confidence for many Indian companies.

Counterfeiting, intellectual property (IP) theft, and piracy currently plague two major industrial sectors — pharmaceuticals and fast moving consumer goods (FMCG). A recent report on counterfeit drugs by the World Health Organization highlighted the nature and severity of this problem¹. In pharmaceutical counterfeiting, the occurrence of even a *single* case is considered unacceptable to society. In addition to placing patients' health at risk and undermining public confidence in medicines, the presence of counterfeit drugs exposes the vulnerability of the pharmaceutical supply chain and jeopardizes the credibility of the entire Indian industry at a time when it is attempting to make major inroads as a global supplier of quality medicines².

The FMCG sector has similarly faced major assaults on brand equity as a result of IP theft. The range of industries and industrial goods that are affected is astonishingly large, from high-end products such as branded cosmetics, fashion accessories, auto parts, and liquor to ordinary low-priced goods that include soaps, chocolates, beverages, and even table salt³. The ease with which counterfeiters have been able to penetrate the market with '*look-alikes*' that are completely indistinguishable from branded products has spread alarm throughout the Indian business community and government circles. A particularly troubling aspect of this problem relates to edible products and beverages. Counterfeit versions, which are manufactured under conditions of poor technical oversight and hygiene, are always of inferior quality to their branded cousins. The fact that counterfeit versions of nearly all edible product brands are rampant throughout India poses a significant risk to the actual owners of the authentic copied brand. The oft-stated lament is that '*we may be just one tragedy away from a major PR disaster*'.

The objective of this manual is not to present a detailed analysis of the counterfeiting problem in India. The senior management of most Indian companies is already painfully aware of both the nature and impact that counterfeiters are exerting on their brand equity, consumer confidence, and financial bottom line. Rather, the purpose in creating this document was to assemble current information on technological solutions that are available to Indian companies and assist them in adopting a sound strategy for protecting their brands through effective technology application. As a result, this manual has been written with the twin goals of pedagogy and advocacy. The manual concludes with a comparison of the various anti-counterfeiting technologies and an objective assessment of which ones are likely to be best suited for the Indian marketplace.

¹ *International medical products anti-counterfeiting taskforce*. WHO Report, 2006. (<http://www.who.int/mediacentre/factsheets/fs275/en/>)

² *Countering Counterfeits*. Pharmabiz Chronicle Special, Interphex India 2007, Mumbai. (<http://www.pharmabiz.com/article/detnews.asp?articleid=40641§ionid=50>)

³ *Counterfeit Branding*. Equitor Management Consulting Report (www.equitor.com/counterfeit.html)

B. Brand Protection — Options and Arguments

At the outset, Indian brand owners have a simple binary choice in terms of counterfeiting — do nothing and let the problem persist, or do something to combat the problem. These two general approaches to dealing with counterfeiting are explored below in greater detail.

1. The *laissez-faire* attitude

The choice to remain passive may be well suited for some companies for various reasons. First, they may not be experiencing an overt attack on their brand or, in some cases, may simply be unaware of the depth and extent of that attack. Unfortunately, in many cases, brand owners are often the last to discover the magnitude and pervasiveness of a counterfeiting problem. In such instances, a *laissez-faire* corporate attitude often arises due to ignorance borne of inadequate market intelligence.

Even if a company is fully aware of the counterfeiting activities on its brands, there may be specific reasons as to why it prefers to remain passive. The following five points represent some of the major causes and/or justifications for inaction.

Counterfeiting is a criminal offence

Some companies believe that counterfeiting is a criminal act and therefore dealing with it should be in the domain of law enforcement. This argument is common within the pharmaceutical industry where the counterfeiting of medicines is a particularly insidious practice. The Indian legislature has recently formulated new laws that impose harsh measures on counterfeiting activities that result in public harm⁴. As a result, some companies take the view that the government should be the proactive entity, rather than the brand owner, in enforcement initiatives. A number of recent anti-counterfeiting conferences in India have focused on the need to usher in greater enforcement of existing laws and called on government involvement toward increased engagement in combating counterfeiting^{5,6}.

Inadequacy of civil jurisprudence

At its core, counterfeiting represents theft of intellectual property and trademark infringement. The implementation of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) by India has mandated greater IP protection and harmonization with global enforcement standards. The currently applicable *Trade Marks Act* provides for greater punishment and fines for counterfeiters⁷. Nevertheless, there remains a general view that prosecuting such civil offences is a lengthy and cumbersome process, often resulting in less than desirable outcomes⁸. This view is compounded by the reality that counterfeiting rarely produces dire consequences in terms of incarceration or redress, and that the perpetrators are often back in society only to become re-engaged in their practices. As a result, some brand owners have become resigned to a mindset that IP theft is simply one of the components of the Indian business environment that must be tolerated.

⁴ *Rajya Sabha passes Bill on spurious drugs with severe penalties*. Article by J. Alexander in Pharmabiz, 2008 (<http://www.pharmabiz.com/article/detnews.asp?articleid=46683§ionid=>)

⁵ <http://www.informedia-india.com/client/Index.aspx?id=conference&sub=program&confID=59>

⁶ http://cii.in/documents/prog_international.pdf

⁷ *Managing your intellectual proficiency: Trade marks*. Report of Business Knowledge Resource Online (http://business.gov.in/manage_business/trade_marks.php)

⁸ *Intellectual property environment in India*. Article by R. Narula (2007) (<http://www.ipfrontline.com/depts/article.asp?id=15279&deptid=6>)

Anti-counterfeiting measures are expensive

There remains a common and pervasive viewpoint among some Indian executives that anti-counterfeiting measures, especially those using innovative technologies, are simply too expensive. The adoption of any such technology will as a result require the company to elevate the price of its goods, which in turn will repel the cost-conscious Indian buyer. This mindset has been particularly reinforced by way of aggressive marketing efforts from companies offering certain anti-counterfeiting technologies, such as RFID and various other taggants, which are indeed inherently expensive to apply at the individual product level. However, as will be evident later in this manual, there now exist entirely new technologies that are highly effective at combating counterfeiting and which are available at extremely low cost.

Corporate bureaucracy and politics

The process of choosing an anti-counterfeiting solution requires evaluation and input from multiple functional units in a company. In general, managers and executives overseeing supply chain, legal, and IT departments become involved in the analytics. For most companies, engaging the marketing department also becomes necessary because the public positioning and portrayal of new technological solutions that impact the consumer requires effective promotional skills and management. The result of this multi-disciplinary engagement is that bureaucratic bottlenecks can often develop within and among the multiple departments.

A further complicating factor is that the cost of an anti-counterfeiting effort is often appropriated from the marketing department's budget, which in turn can set up a conflict of purpose. Whereas the outcomes of routine marketing investments are tangible and immediate in terms of promotional impact and sales growth, the benefits of adopting anti-counterfeiting measures are more long-term in nature and benefit the corporation as a whole. Marketing executives are psychologically driven to undertake efforts that boost sales and provide immediate rewards for their department. An expenditure of time and energy, not to mention a portion of their budgetary allocation, toward combating counterfeiting simply does not fit the political goals of such a mindset. This is particularly so when the eventual success of their anti-counterfeiting investment is glorified at an institutional rather than a departmental level. Consequently, the adoption of major anti-counterfeiting initiatives has generally occurred in a top-down manner at corporations that have senior executives with the resolve and foresight to protect their brands.

Uncertainty on the optimal solution

The international marketplace is currently brimming with various types of brand protection technologies. As a result, it is not an easy task to fully fathom the capabilities and drawbacks of the various anti-counterfeiting solutions to arrive at a confident decision. Given the difficulty in sorting through the myriad available technologies and the limited bandwidth of corporate executives, a *laissez-faire* approach often becomes the default position for many companies.

A key goal in assembling this manual was to provide a comprehensive appraisal of the strengths and weaknesses of currently available solutions, and thereby provide the due diligence that would normally require much time and effort for Indian brand owners in evaluating the various anti-counterfeiting technologies.

2. The *proactive* approach

An entirely different viewpoint can be found among brand owners who are determined to combat their counterfeiting problem. The proactive approach taken by some companies has involved a varied set of strategies. Indian companies, until recently, were limited in their choice of available technological solutions and therefore generally relied on applying holographic labels as a security feature. This solution can be found in several product lines, especially pharmaceutical packaging⁹. Another approach taken by some companies was to modify their packaging entirely from time to time in order to keep one step ahead of the counterfeiters. Some companies have also undertaken direct interdiction efforts by either setting up their own security division or contracting a third-party agency to keep vigilance on the market and undertake raids when necessary¹⁰.

The argument for taking a robust proactive view to counterfeiting is based on the notion that no one other than the corporate owner is really interested in protecting their brand equity. The following are some influential arguments that motivate brand owners into taking an aggressive stand against counterfeiting.

Financial loss

It is unquestionably true that IP theft represents a foremost source of revenue loss, especially for those companies whose major-name brands have been targeted. The public domain is replete with various studies and accounts on the financial impact of counterfeiting. Data from official sources and informed estimates on the overall magnitude of this problem are depressingly bleak, and do not require repetition in view of the various accounts that are already available^{11,12}. The loss suffered by some individually named companies in various studies is especially troubling — 1,000 crores annually for a leading Indian FMCG company and anywhere from 10% up to 30% of the sales of certain major brands across various product categories¹³. It is this type of erosion on the bottom-line that drives many corporate executives, either at their own initiative or under pressure from their Boards and shareholders, to examine and undertake robust strategies for protecting their brands and reducing the monetary loss from counterfeiting.

Government pressure

Revenue loss is not just restricted to the brand owner. It is axiomatic that counterfeiters do not pay taxes and as a result, various state and central government agencies incur significant loss due to tax evasion. This problem is particularly acute in certain product segments — e.g., liquor, luxury goods, imported items, etc. — where the margin markup due to excise and other forms of taxes actually accounts for a significant portion of the MRP. To mitigate this loss, governments have begun to place considerable pressure on various industries to implement anti-counterfeiting strategies. In some cases, certain state governments have even begun to take the initiative themselves by applying anti-counterfeiting technologies on their excise stickers and other tax stamps¹⁴.

⁹ *Hologram case study*. Report by hologram suppliers trade group. (<http://www.hologramsuppliers.com/case-study.html>)

¹⁰ *Companies hire private agencies in India to take on counterfeiters*. Article by K. Merchant, Los Angeles Times, 2004 (<http://articles.latimes.com/2004/aug/02/business/ft-counterfeit2>)

¹¹ *India facts and figures*. Report of the International Chamber of Commerce, 2006. (<http://www.iccwbo.org/bascap/id7852/index.html>)

¹² *Indian piracy industry packs a \$4 bn punch*. Article by N. Verjee, The Wall Street Journal, 2008. (<http://www.livemint.com/2008/03/24001613/Indian-piracy-industry-packs-a.html>)

¹³ *Countering Counterfeits*. Report by G. Sridhar presented at International Marketing Conference on Marketing & Society, 2007. (<http://dspace.iimk.ac.in/bitstream/2259/313/1/737-742.pdf>)

¹⁴ Press release by Holostik India Ltd., 2005 (http://www.holostik.com/about_press.html)

A second form of pressure from government circles for more aggressive implementation of anti-counterfeiting measures relates to fundamental issues around consumer safety, economic progress, and even the national image¹⁵. An excellent example is the recent widespread and unrelenting negative publicity that followed a major incident of tampering on a commonly used anti-coagulant drug. The global media spotlight was not only devoted to the product itself but also in nearly every instance named the country of origin for the problem¹⁶.

Regulatory compliance

Indian brand owners are becoming particularly mindful of the regulatory environment that is emerging in the global business arena. International treaties and regulatory impediments by various national governments will eventually impose restrictive conditions for importation of various products. A number of highly publicized recent cases of counterfeit products originating from China have highlighted the need for greater public protection in various Western markets and have propelled calls for legislative action. One example is the European Commission's proposal to negotiate a new *Anti-Counterfeiting Trade Agreement* (ACTA) with major trading partners¹⁷. Although the governing framework for this agreement has yet to be adopted, and it is not yet clear how it may impact Indian business, a protectionist move is clearly unfolding as a result of public pressure to ensure that consumer goods are protected throughout the entire supply chain cycle.

One industry that will soon have to comply with new regulatory requirements abroad is the pharmaceutical sector. The Food and Drug Administration (FDA) in the United States recommended implementation of robust supply chain tracking for all medicines in 2004¹⁸. The State of California has responded with a new law (SB 1476) that imposes stringent requirements for drug importation and sale, to the point where anti-counterfeiting measures must encompass medicines right down to the single item level¹⁹. There are now several additional states that have imposed similar laws, with the expectation that a national measure will soon be in place. The European Commission has also expressed alarm at the magnitude of pharmaceutical counterfeiting and has singled out India as the major source of fake drugs confiscated by its customs officers²⁰. The European Federation of Pharmaceutical Industries and Associations (EFPIA) has followed through and also

What is SB 1476?

The State of California has passed a bill (SB 1476) that was signed into law by Gov. Schwarzenegger requiring all drugs sold in that state to have passed through a secure supply chain system and to also have an electronically documented trace of that drug's movement, referred to as the electronic pedigree (*e-pedigree*). All prescription medicines must be **electronically** tracked and traced at all times throughout the complete supply chain, according to this law. The stringency is such that even the smallest packaged medicine must adhere to this requirement and actually have an e-pedigree. The law was to take effect at the start of 2009. However, industry pressure led to a two-year reprieve, with the start date of this requirement now being moved to **January 01, 2011**. Indian pharmaceutical companies currently exporting to the U.S., or planning to do so in the future, will be frozen out of this market if they are not in compliance.

¹⁵ Special address by Shri Navin Chawla, Secretary, Ministry of Consumer Affairs, 2004 (<http://www.ficci.com/media-room/speeches-presentations/2004/apr/apr21-piracy-navin.htm>)

¹⁶ *The Drug Scare that Exposed a World of Hurt*. Article by W. Bogdanich, New York Times, 2008. (http://www.nytimes.com/2008/03/30/weekinreview/30bogdanich.html?_r=1&oref=slogin)

¹⁷ *Intellectual property fact sheet: anti-counterfeiting trade agreement*. Report from the European Commission. (http://ec.europa.eu/trade/issues/sectoral/intell_property/fs231007_en.htm)

¹⁸ *Combating Counterfeit Drugs: A report of the Food and Drug Administration, 2004*. (http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html)

¹⁹ Background and Summary of the California ePedigree Law. (http://www.pharmacy.ca.gov/laws_regs/e_pedigree_laws_summary.pdf)

²⁰ *Summary of Community Customs Activities on Counterfeit and Piracy*. Report of the European Commission Taxation and Customs Union

recommended strong anti-counterfeiting protection before allowing drugs manufactured abroad to enter into European markets.

In view of these emerging developments, many executives in the Indian pharmaceutical industry realize the urgent need to implement robust anti-counterfeiting measures to preserve their export markets, and be prepared for the possibility that similar policies may eventually be introduced in India. The potential jeopardy for Indian companies is that if such measures are not enacted, then their drugs will simply not be permitted entry into major Western markets. In addition to the immediate business loss, the vacuum created by such barriers will be filled by other vendors who have implemented the needed anti-counterfeiting measures.

Consumer confidence

Another issue that serves to motivate a proactive approach amongst brand owners concerns the very people who purchase their products. Customer loyalty is a coveted component of brand consumerism, something that is difficult to establish and requires considerable marketing investment and retail presence. The loss of brand reputation and consumer goodwill is therefore all the more painful. Several brands in the Indian marketplace have been around for decades and have established their name only through sustained effort and creative marketing strategies. Others, belonging to major multinational corporations, have been launched in India after having become blockbusters in overseas markets.

There are two concerns that are foremost in the minds of modern consumers — product safety and purchase value. Counterfeiting can have different impacts in each of these areas depending on the nature of the product. For example, medicines, edible products, and generally any item associated with babies generate an inherently high psychological sensitivity with regard to product safety. On the other hand, products that cater to lifestyle and luxury are more prone to concerns regarding purchase value and whether or not the brand-name item that has just been bought is truly genuine. It is therefore unassailably true that Indian manufacturers across a broad spectrum of consumer products should have a singular goal of reassuring their customer base and retaining confidence in the brand²¹. An emerging view of the best way to attain that goal is for brand owners to take proactive steps in combating counterfeit attacks on their brands and empower their customers with the ability to authenticate their purchase²².

Corporate social responsibility

An oft-expressed viewpoint is that government agencies can be proactive in adopting tough laws and create public awareness, but the brand owner must ultimately take the in protecting their own products in the marketplace. The motivation to do so for brand owners is self-interest as well as the safety of their consumers. The 'self-interest' factor arises from protection against blame being placed upon them for not taking steps to help consumers identify a genuine product. In such circumstances, the potential public relations damage can easily outweigh any direct compensatory claims in the event that a counterfeit product leads to public harm. The simple question of *'what did you do to protect me?'* can be easily leveled against derelict brand owners who had the foreknowledge that their products were under attack from counterfeiters.

(http://ec.europa.eu/taxation_customs/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/counterf_comm_2006_en.pdf)

²¹ *Counterfeiting of goods: Loss in reputation and goodwill*. Article by MS Nair, Mondaq Business Briefing, 2006. (<http://www.mondaq.com/article.asp?articleid=39288>)

²² *The role of authentication technologies in counterfeiting*. Article by IM Lancaster for World Intellectual Property Organization, 2006. (http://www.wipo.int/wipo_magazine/en/2006/02/article_0004.html)

This potential jeopardy can be particularly worrisome for those manufacturers in sensitive product segments — e.g., edible items, infant and children's products, cosmetics and beauty care, and medicines. There have been numerous recent instances of tainted products from China that point to the sensitivity surrounding edible products²³, including a particularly odious case of counterfeit baby formula²⁴. Although India has been largely spared from highly visible examples of such negative publicity, the many instances here of known counterfeiting on branded food and beverage products have produced a worrisome situation within the industry and motivated many companies to examine the application of anti-counterfeiting technologies.

One industry that has been particularly vulnerable is the pharmaceutical sector. The best-case scenario for a counterfeit drug is that it does not produce the desired therapeutic effect, while the worst-case scenario is that it harms or kills the consumer. There is no dearth of examples in this regard from both India and abroad²⁵. Consumer groups have advocated the position that brand owners must protect their products and take all necessary measures for both clinicians and consumers to identify a bonafide drug. Although there are no guarantees that a particular drug will not be faked and sold in the open marketplace, the argument that pharmaceutical companies must make genuine efforts to protect their products has now gained widespread acceptance²⁶.

Competitive edge and market share

Another argument for taking a proactive anti-counterfeiting approach is with regard to retaining (and increasing) market share. Counterfeiters are not the only ones who threaten brand value and sales. All major brands are also under constant pressure from legitimate competitors, whether existing companies (*incumbents*) or new entrants (*attackers*). In the event that one of the competitors should implement an anti-counterfeiting technology in their product line, a strong marketing advantage turns to their favour in terms of offering enhanced consumer safety and purchase value. Depending on the marketing skills of the competitor, this advantage can serve as a highly effective stimulus to increase market share and thereby depress sales of other companies in the same segment who have not embraced an effective program of product security and consumer communication²⁷.

In such circumstances, the derelict companies will face the burden of having to quickly initiate a similar anti-counterfeiting program to maintain parity in the marketplace and offset the advantage accrued by the competitor. The jeopardy here is that any technology implementation is a slow and cumbersome process for most major companies. Therefore, by the time that corrective measures have been taken, the competitor has already had a significant head start in the marketplace and secured considerable sales and marketing advantages. For this reason, brand owners in highly competitive sectors — such as cosmetics & beauty care, snacks & beverages, infant & children's products, the electronics industry, and pharmaceuticals, among others — have already begun to evaluate the application of robust new anti-counterfeiting technologies to their product line²⁸.

²³ *Tainted Chinese Imports Common*. Article by R. Weiss, The Washington Post, 2007.

(http://www.washingtonpost.com/wp-dyn/content/article/2007/05/19/AR2007051901273_pf.html)

²⁴ *Fake Milk Powder Causes Baby Death*. Report in CBS News, 2004.

(<http://www.cbsnews.com/stories/2004/06/09/health/main622021.shtml>)

²⁵ *Bad Medicine*. Article by R. Bate in The American, 2008.

(<http://www.american.com/archive/2008/may-june-magazine-contents/bad-medicine>)

²⁶ *The Global Threat of Counterfeit Drugs: Why Industry and Governments Must Communicate the Dangers*. Article by R. Cockburn et al. in PLoS Medicine, 2005.

(<http://medicine.plosjournals.org/perlserv/?request=get-document&doi=10.1371%2Fjournal.pmed.0020100>)

²⁷ *Counterfeiting and the Art of Deception*. Article by M. Bennett in BP Council, 2008.

(<http://www.bpcouncil.com/apage/printv/555.php>)

²⁸ Based on feedback from a cross-section of Indian companies who were contacted across different product

Being prepared

A final argument that is often expressed among the more proactive group of brand owners is to ensure preparedness in the event that a counterfeiting onslaught should target their products, which were previously immune to such attacks. There are indeed very few major brand owners in India who are in this enviable position. Some companies that currently enjoy and operate in a "counterfeit-free" business environment may not see an immediate urgency to become preoccupied with anti-counterfeiting solutions. The same applies to companies who are entering India with new products. For both groups, there is a high probability that their brands will become targeted at some point. Regardless of the risk foreseen in the marketplace, a viewpoint often advocated by counterfeiting experts is to take a protectionist approach, for the simple reason that an investment which shields their coveted brands is a wise and prudent business decision²⁹. For some brand owners, this decision may be reached at a relatively mature point in the life cycle of a product, whereas for others it may be at the point of entry into the Indian marketplace.

segments in the preparation of this document.

²⁹ http://findarticles.com/p/articles/mi_m0EIN/is_2006_Oct_26/ai_n27028684

C. Choosing the Right Technology — The Five Golden Qualities

When evaluating anti-counterfeiting technologies, two questions generally remain foremost in the minds of corporate executives: *'will it work?'* and *'will it be worth the investment?'*. These questions are particularly germane in view of disappointing results that some companies have experienced in their rush to adopt various methods to protect their brands, only to see that astute counterfeiters were able to defeat their efforts in short order. The key issue therefore is not simply to adopt *a* technology, but to adopt the *right* technology.

The application of an anti-counterfeiting solution can indeed provide excellent protective measures and significantly reduce (and even defeat) the counterfeiting problem if the brand owner adopts three fundamental strategies. First, the solution must be thoughtfully chosen; second it must be effectively promoted in the marketplace; and third, the technology must be properly implemented. These three core strategies are reviewed in reverse order.

First, in order for any technology to succeed, it must be implemented at the most elemental level — i.e., the very product that is sold in the marketplace. Brand owners must therefore focus their efforts only on those solutions that empower product-level authentication. The greatest success in terms of interdiction and deterrence against fraud can only occur when a brand owner's products are clearly distinguishable from counterfeits and knock-offs. The role of the technology solution should be to greatly facilitate that distinction, which in turn provides a clear asset in terms of an anti-counterfeiting impact.

The second fundamental strategy requires the brand owner to communicate its adoption of an anti-counterfeiting solution to the marketplace. Although this should seem obvious, many brand owners are loath to admit that a counterfeiting problem had afflicted their products in the first place. This dilemma can be effectively handled by a creative marketing department that publicly portrays a brand protection solution, not in terms of an anti-counterfeiting objective, but rather in terms of brand evolution that is in the best interests of protecting the health and safety of their consumers. This positive approach makes a far more effective message. Ultimately, the single most important mechanism for detecting a fake product is quite obvious but has been largely overlooked — *you have to check it!* The brand owner will be remiss if it invests in an anti-counterfeiting technology and then fails to properly promote it in the marketplace.

The third and final strategy is elegantly simple — choose the right technology! Some companies in the past have deployed a technology solution that did not effectively target the actual problem and therefore ended up being unsuccessful, much to the consternation of senior management. For example, certain anti-counterfeiting technologies are inherently expensive but have a short half-life because the counterfeiter can easily duplicate them. An effective solution for protecting branded assets can only be arrived at by identifying a technology that has considerable robustness and longevity, and yet requires a modest and acceptable level of investment.

So, how exactly does a brand owner confidently identify a brand protection technology that will have a high probability of success in passing the two salient questions posed at the outset — *will it work and will it be worth the investment?* There are five Golden Qualities that are critically important in any effective anti-counterfeiting solution. These are discussed in the remainder of this section. The brand owner must ensure that a chosen technology displays as many of these as possible, but at the very least, incorporates the first three Golden Qualities.

1. Consumer empowerment

A fundamental requirement for brand owners is to adopt a technology that can be applied at the individual product or item level, as noted above. This does not, however, automatically mean that consumers are capable of using that technology to distinguish a genuine from a fake product. There are various brand protection solutions that are indeed applied at the product level, but which are of use only to security specialists and therefore impenetrable to the ordinary consumer. The first Golden Quality that must be assiduously sought by the brand owner is a solution that empowers their customers to authenticate at the very moment when it is most important — the point of sale at the retail level.

Consumer empowerment represents an absolutely critical requirement for several reasons. First, any brand protection technology meant to reassure consumers misses its key objective if the customer is unable to use that very technology. The twin aspects of reassurance in this regard pertain to product safety and purchase value, both of which are necessary for retaining brand loyalty, growth, and confidence. Second, a strong case can be made in terms of obtaining a marketing edge when consumers are empowered with verification ability. The technology can be publicly portrayed in an extremely positive manner because it reinforces an important psychological aspect of brand consumerism — giving power to the masses. Third, consumer verification at the time of purchase serves as the most potent answer to public calls for greater corporate responsibility and provides the best response to that delicate question directed at the brand owner — *'what did you do to protect me?'* The anti-counterfeiting technology in this case would not only provide robust brand protection but also shield the owner from any culpability in those cases where a fake product was purchased by a consumer who opted to bypass verification. Fourth, consumer empowerment serves as a strong deterrent to wayward retailers who are themselves part of the counterfeiting loop. The identification of fake goods at the point of sale would provide an entirely new dilemma and make guilty retailers aware that they can be easily identified as perpetrators of criminal activity, while rewarding honest ones for diligently selling authentic products. And finally, consumer empowerment marshals a very large field-force of independent invigilators to combat the counterfeiting problem. The brand owner benefits by enlisting a truly incredible resource that is extremely large in terms of sheer numbers, broad in terms of geographic scope, and which requires no additional expenditure, as would be the case, for example, in hiring an equally large security firm to undertake random authentications throughout the country.

In short, there is an extreme level of significance to the brand owner in adopting a technology that empowers consumer authentication, as noted by way of the various reasons outlined above. For this reason, consumer empowerment represents a core Golden Quality. Any anti-counterfeiting solution that fails to provide this critical feature should only be adopted if there are compelling product-specific reasons that mitigate this requirement.

2. Cost and value

The investment needed for implementing an anti-counterfeiting solution is a complex issue and represents a concern largely driven by corporate matters specific to each individual company. For example, if a brand owner is being battered to the point where its branded assets are becoming devalued in the marketplace, then the cost of the anti-counterfeiting solution becomes assessed in relation to the loss being incurred³⁰. Alternatively, a brand owner that has been relatively immune may also opt to invest heavily in anti-counterfeiting measures because the path to product development and market penetration had required significant corporate resources or global brand imprinting.

³⁰ *Security Labeling*. Article by L. Genuario in *Label & Narrow Web*, 2004.
(<http://www.labelandnarrowweb.com/articles/2004/11/security-labeling>)

An opposing viewpoint of fiscal restraint applies to those sectors that are restricted in their ability to pass on additional costs to their consumers by way of price escalation, and therefore the financial impact of an anti-counterfeiting solution becomes a sensitive issue. This concern is particularly germane to companies whose products are in extremely competitive markets or those that are regulated by the government. The pharmaceutical industry represents the best example in terms of the latter category, where the National Pharmaceutical Pricing Authority (NPPA) decrees the market price of many medicines. In view of the widespread concern over pharmaceutical counterfeiting in India, it is likely that cost recovery by way of a modest price increase for implementing anti-counterfeiting measures would be permissible. The NPPA can reduce the prices of drugs but also increase them when it is responsible to do so³¹.

The cost of anti-counterfeiting technology therefore represents an essential consideration in the path to choosing the right solution. The Golden Quality in this case is simple and represents one of the cornerstones of the business world — find a solution at the lowest cost and which offers the highest value proposition. There are no well-defined parameters as to how much a technology solution should cost when considered at the single item level, and therefore examined strictly in relation to the product's market cost. Some esoteric anti-counterfeiting solutions can cost upward of 10 rupees per protected product, and therefore are clearly not suited for low-cost brands. On the other hand, some low-cost solutions may not offer sufficient protection because the counterfeiter can easily duplicate them. The value proposition in such cases is extremely low in terms of robustness (i.e., difficulty in duplicating the technology). This is disconcerting because the capital investment made in applying the solution becomes a loss proposition for the brand owner, where the technology soon becomes either useless or obsolete in terms of brand protection.

The two pricing issues that brand owners must carefully sort through are capital investment and residual cost. There are no technologies that are entirely devoid of an initial investment because product-level implementation will inevitably require either new equipment acquisition or some modification of an ongoing production process. Residual cost refers to the actual implementation cost per product sold in the marketplace. One practical rule of thumb is that the technology cost should ideally be in the range of 0.1 - 1.0% of the current *maximum retail price* (MRP) for that product. Any cost beyond this range will be difficult to bear for most brand owners due to various strategic considerations, most importantly keeping their product competitive in the marketplace. After all, consumers want the best of both worlds — product protection without significant cost escalation.

The second Golden Quality, therefore, requires the technology offering to be of low cost in terms of capital investment and running cost, and yet maximally offer the other Golden Qualities listed in this manual. The challenge for the brand owner is to find a technology that does not exceed the 1% rule, and ideally at an even lower cost, and yet offers an excellent value proposition. The various currently available anti-counterfeiting technologies will be later assessed in this regard.

3. Forensics and interdiction

The deployment of an anti-counterfeiting technology by a brand owner is made with a singular goal — to reduce or eliminate counterfeiting and piracy in the marketplace against their branded products. This is maximally accomplished when the technology provides sufficient deterrence that makes it risky for the counterfeiter. Deterrence, in turn, is a result that occurs only when the technology empowers interdiction by police and security officers. Interdiction, in turn, is an outcome that only arises if the technology has sufficient forensic

³¹ NPPA revises prices of 149 formulation packs. Article in Pharmabiz, 2008. (<http://www.pharmabiz.com/article/detnews.asp?articleid=46403§ionid=>)

applicability. Without that, an anti-counterfeiting solution is neither a solution nor does it effectively combat counterfeiting. This is precisely why brand owners in the path to making their choice must assess the forensic capability of a technological solution.

This may seem like a daunting task, and well outside the capabilities of many corporate executives and managers. However, the answers to a few simple questions are all that is needed. First, does the technology effectively differentiate a genuine from a fake item? All anti-counterfeiting solutions must pass this first level, and one does not need to have security expertise to make this determination. Second, can the technology be utilized directly at source, i.e., where the product is sold, to verify its authenticity, or does the product have to be taken to a laboratory for forensic analysis? Those technologies falling in the latter category should be avoided because the deterrence factor then becomes devalued. Counterfeiters and their retail partners can either relocate or simply go into hiding. A technology that empowers point-of-sale authentication provides the greatest deterrent effect. Third, does the technology permit consumers with failed verifications to communicate this information to the brand owner, their security agency, or a police force? There are new computerized technologies that actually undertake this operation automatically and alert the brand owner when consumer authentication failures occur, along with key information on the place, date, and time of the counterfeit intercept. And finally, can the technology be effectively used for prosecution? All major brand owners have a legal department that should be involved in making this assessment based on input from potential technology providers.

The third Golden Quality therefore requires that an effective anti-counterfeiting technology must have robust forensic applicability, and which is ideally effectuated at the retail level. Brand owners will be rewarded by implementing those technologies that meet this requirement because of a simple fact of the human psyche — thieves do not like to get caught and when faced with a new technology that poses an interdiction threat, they will simply move on to other vulnerable products.

4. Simplicity and adaptability

The fourth Golden Quality concerns the properties of the anti-counterfeiting technology that ensure ease of implementation, use by the consumer, and long-term stability. Brand owners will spontaneously seek to apply those solutions that cause minimal disruption in the product manufacturing process. Some anti-counterfeiting technologies require significant intrusion at the plant level whereas others can be implemented with greater ease. It is rarely the case that any given technology provider will have an in-depth knowledge of the manufacturing process or what application strategies are best likely to work for a particular branded product.

The exact mode of application and the best solutions in this regard are highly product-dependent. Brand owners must therefore work closely with technology providers to arrive at an optimal implementation solution. Given the investment that is often required on the part of the brand owner, one path to arriving at a confident solution may involve undertaking a pilot project. This can be devoted to one particular brand in the company's product portfolio, a particular manufacturing plant, a specific geographic location, or some other filter that reduces the up-front commitment to adopt a specific technology and yet provides for an effective mechanism by which to evaluate that technology.

Once a particular technology is chosen, it is highly likely that the brand owner will be married to that solution for quite some time. During that period, the brand will certainly evolve and new requirements may be imposed, such as package modification, new marketing challenges, growth (or diminution) of sales, brand offshoots, altered manufacturing practices, new regulatory requirements, and various other unforeseen

events. The best anti-counterfeiting technology in such circumstances is one that is highly adaptable and therefore can meet most new requirements. Technological adaptability also assures longevity because the technology can change with the times and needs of the brand owner.

5. Value-added features

All brand owners seek additional features that can be bundled into any newly acquired technology so that they are able to leverage their investment into other business areas. The same would be the case when adopting an anti-counterfeiting technology. The goal here would be to see what other applications or value-added features are provided by the technology in addition to combating counterfeiting. Although the main driver behind adopting a specific technology is to maximize brand protection, any other benefits offered by the same technology make it that much more appealing across a wider segment of the company's operational landscape.

There are three potential applications that can be considered as value-added features in this regard. The first concerns marketing and promotional tools. Brand owners face constant challenges in optimally positioning their products in a competitive marketplace, whether in terms of new product introductions, spin-offs from existing power brands, or simply finding creative new ways to expand their customer base. Given that an effective anti-counterfeiting technology must be implemented at the product level, those technologies that are also effective in empowering consumers can provide a communication portal as well. This is particularly true for a new genre of electronic anti-counterfeiting technologies, as discussed later in this manual.

An associated advantage is that some technologies even provide feedback to the brand owner as to the date, time, and place of the authentication. As a result, the brand owner is able to gather market intelligence and see how their sales are unfolding in real time, as well as identifying geographic zones that are especially successful and those that are lagging behind. FMCG companies generally have to invest heavily in order to obtain such market intelligence and therefore any anti-counterfeiting technology that provides this information would represent a coveted value addition.

A final feature that is especially important in the context of an overall anti-counterfeiting strategy is a solution that additionally provides supply chain tracking ability, also known as *Track & Trace* technology. Certain anti-counterfeiting solutions are deficient in this regard whereas for others, this is a core component of the technology itself. In the latter case, the supply chain management tools can be used at the discretion of the brand owner to track the movement of goods, to maintain inventory, to keep tabs

What is *Track & Trace* technology?

Track & Trace is the process of recording the past and present whereabouts of a shipment as it passes through different handlers on its way to its destination, through a distribution network. Typical applications for *Track & Trace* are to identify where a product was "diverted" from its intended course (parallel importing) or where a fake product was introduced.

The *Track & Trace* concept is usually supported by means of reckoning and reporting of the position of the vehicles that are transporting containers with the property of concern in real-time. Another approach is to report the arrival or departure of the object and recording the identification of the object, the location where observed, the time, and the status.

International standards are now in place that codify the syntax and semantics for supply chain events and the secure method for selectively sharing supply chain events with trading partners, such as the electronic pedigree (*e-pedigree*). These standards for *Track & Trace* have been used in successful deployments in many industries and there are now a wide range of manufacturing and distribution processes that are compatible with these standards.

Source: Wikipedia
(http://en.wikipedia.org/wiki/Track_and_trace)

on any diversions, to undertake recalls when necessary, and to comply with regulatory requirements. Emerging trade regulations will soon mandate a *Track & Trace* requirement for product importation in various countries. One industry that is immediately affected in this regard is the pharmaceutical sector due to the imminent requirement in some markets for an *e-pedigree* for every medicine right down to the unit level. The supply chain management tool in this case must be able to generate such a report in electronic form to satisfy drug regulators in the U.S. and other countries soon to follow.

The fifth and final Golden Quality refers to anti-counterfeiting technologies that provide additional valuable features, whether by way of capitalizing on their consumer outreach aspects to offer new avenues for brand marketing and promotion, obtaining sales information or other market intelligence, or as a supply chain management tool. The more value-added features that are offered by the technology, the greater will be the set of applications at the disposal of the brand owner. In such cases, the technology becomes integrated into a broader segment of the company's operations and helps promote the brand in ways that are supplemental to providing robust anti-counterfeiting protection.

D. Currently Available Anti-Counterfeiting Technologies

The primary objective of any anti-counterfeiting technology is to empower someone — a consumer, a security agent, a government official — to authenticate a product and thereby ensure that it is the genuine article. There is a long history of attempts at combating counterfeiting and along the way, various types of authentication technologies have been developed and applied with mixed success. Some of the newer technologies are extremely sophisticated and can be very effective. However, it is the computer-based solutions that are creating the greatest exuberance in the field of product security^{32,33}.

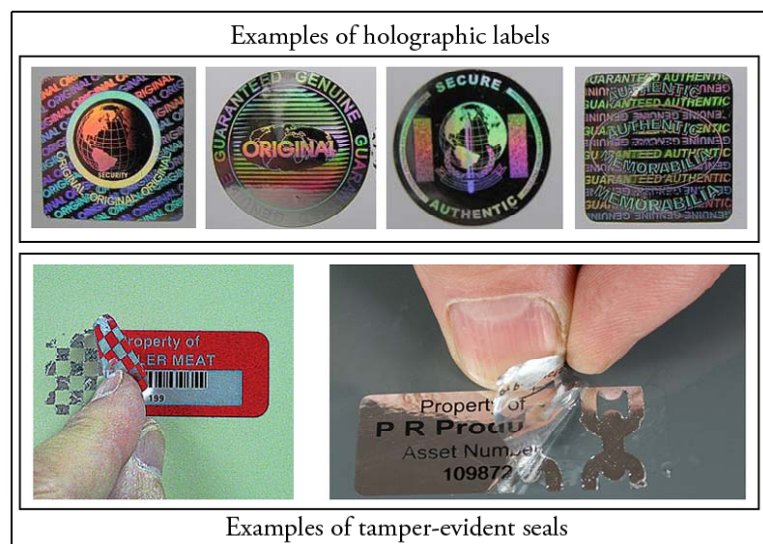
The current landscape of anti-counterfeiting solutions presents a mind-boggling array of technologies in terms of both sheer number and variety. It would be a major exercise for any company to have to sort through all of the technology offerings. A key objective in writing this manual, therefore, was to provide Indian brand owners with a succinct overview of the brand protection solutions that are currently at their disposal. This is a task, however, that can be greatly facilitated by streamlining these technologies. It turns out that all anti-counterfeiting solutions can be placed into one of three major categories. The discussions that follow revolve around these three categories, with further sub-classifications within them based on any additional distinguishing characteristics.

1. Passive technologies

The first category of anti-counterfeiting technologies concerns those that allow a genuine product to be distinguished only by visual inspection. In other words, no special devices or readers are needed. This category is referred to as *passive technologies* and includes three sub-categories, as discussed below. In all cases, the technology is applied directly onto a branded product, which then allows a customer to use its presence as a means of verification, and thereby presumes the product as being authentic. The advantages and disadvantages of these technologies are taken up briefly in each subsection below, and also later in Section E where a head-to-head comparison is made between all of the major anti-counterfeiting technologies discussed in this manual.

a) Holograms and security seals

The science of holography dates back to the post-War era of the late 1940s when it was originally developed. The creation of a holographic image, or hologram, requires some technical knowledge and expertise³⁴, though a recent explosion of companies and low-cost machinery has made this technology extremely accessible within many sectors of the consumer marketplace. A hologram typically incorporates an image that appears as an illusory 3-dimensional object with vivid depth characteristics.



³² *How the pharmaceutical industry is pushing supply chain technology.* Article by T. Aniel in Modern Materials Handling, 2008. (<http://www.mmh.com/article/CA6515573.html>)

³³ *Electronic pedigree and Authentication Issues for Aerospace Part Tracking.* Article by M. Harrison & A. Shaw, University of Cambridge, 2006. (http://www.aero-id.org/research_reports/AEROID-CAM-001-Pedigree.pdf)

³⁴ *About Holograms – How a Hologram is Made.* (<http://www.holograms.bc.ca/home2.htm>)

A *security hologram* is a special reflective type of hologram that is custom-made for a brand owner. The most familiar holograms are those found in credit cards, currency notes, medicine packs, and various consumer goods. A number of Indian brand owners have relied on hologram application as a means to reduce counterfeiting, especially in the pharmaceutical industry³⁵. There are currently a large number of hologram suppliers in the global marketplace, led by major companies that have an Indian presence, such as DuPont, Kurz, and Tesa Scribos. Additionally, there are over two dozen Indian manufacturers of security holograms. The commercial interests of these companies are represented by their trade organization, the Hologram Manufacturers Association of India (HoMAI)³⁶.

A common way to apply a hologram onto a product is by way of a security seal or label. There are many different types of security labels in the marketplace, all of which allow brand owners to place a distinguishing feature on their products. One particular type of security seal that can be used in conjunction with a hologram is the so-called tamper-evident label. Such labels require one part of the seal to be removed to display a message or security code. Once removed, the two parts of the label cannot be reattached and therefore provides clear evidence that the product has been tampered with. The argument behind using tamper-evident and other types of security seals as an anti-counterfeiting tool is that they generally contain a special engraving, message, code, or holographic image that sets the brand owner's products apart from those belonging to an imposter.

The advantages that holograms and security seals offer is that they are generally of low price, easy to apply, and represent a rapid way of providing a distinguishing feature to a branded product³⁷. The major disadvantage is that this solution is easily replicable by a counterfeiter, and indeed, there have been numerous instances where genuine security holograms have been easily and expertly copied or simulated³⁸, leading to the contention that holograms when used alone are less about security and more about sparkle³⁹. An additional difficulty relates to consumer awareness. With a plethora of branded products in the marketplace, the average consumer has an extremely difficult time keeping up with which products should contain a particular type of hologram or seal. Related to this is the fact that fake holograms used by counterfeiters, though of inferior quality, are not easily distinguishable as such by the lay consumer.

b) Overt and hidden imaging

A second type of passive technology is associated with special types of imaging that can be applied either in an overt (visible) or semi-covert (hidden) manner on a product or label. Again, the justification here for use as an anti-counterfeiting tool rests on the claim that such specialized features are specific to a branded product and therefore serves to distinguish it from a fake one. As with holograms, the use of these technologies is reliant entirely upon a consumer being able to know and visibly detect the presence of this feature on the product, hence their classification as a passive technology.

There are several different options in this category. One is to apply an optically variable device (OVD), which is similar to a hologram but without a 3D component. These

³⁵ *Trends: Holograms and Anticounterfeiting*. Article by I. Lancaster in PharmaTech, 2008. (<http://pharmtech.findpharma.com/pharmtech/In+the+Field/Trends-Holograms-and-Anticounterfeiting/ArticleStandard/Article/detail/505361>)

³⁶ HoMAI – Hologram Manufacturers Association of India. Promotional piece in BPCouncil, 2007. (<http://www.bpcouncil.com/aws%20alphabetic%20presentation/c116/2346.php>)

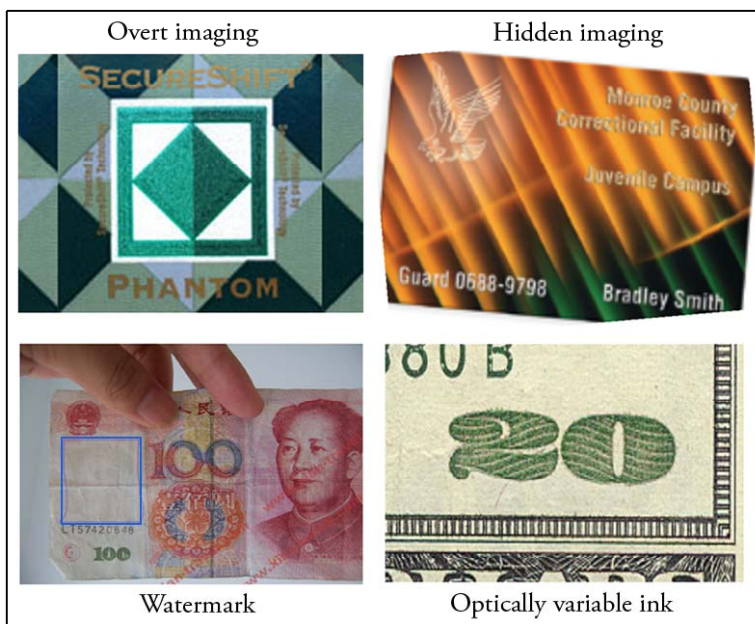
³⁷ *Counterfeiting – Lines of Defence*. Article by R. Mistry in Pharmabiz Chronicle, 2007. (http://www.holotechonline.com/counterfeiting_Lines.html)

³⁸ *Anti-counterfeit Technologies for the Protection of Medicines*. Report of the World Health Organization. (<http://www.who.int/impact/events/IMPACT-ACTechnologiesv3LIS.pdf>)

³⁹ Article by M. Graham in Wired Magazine. (<http://www.wired.com/science/discoveries/news/2007/02/72664?currentPage=all>)

overt images are made on transparent film, which serves as a carrier, and then placed on a reflective backing layer to produce different visual impressions, such as image flips, transitions, color shifts, or a floating sensation. The 3M Corporation is a leading manufacturer of this technology⁴⁰ and has recently undertaken a major effort to expand its commercial presence in the Indian pharmaceutical marketplace⁴¹.

The other technology offerings in this category concern semi-covert or hidden image features that require a small additional effort on the part of the consumer to detect their presence. There are a variety of possibilities in this regard, including embedded images that are only visible from one particular angle of view, digital watermarks, and optically variable inks (OVI). The latter two are often applied on sensitive documents and have been used in various worldwide currencies. Watermarks, for example, have now become quite common in currency, such as the image of Mahatma Gandhi in Indian rupee banknotes. OVI, which is also known as colour-shifting ink, is a particularly intriguing technology because it changes color as an object is rotated. An example is United States currency, where the dollar amount is printed with OVI. The major provider of OVI technology, which also has an Indian presence, is the Swiss company SICPA SA⁴².



The advantages of this group of passive technologies are that they are easily applied onto branded products, and especially documents. The result is an esthetically appealing end-result that can incorporate highly specific iconic images that are unique to the brand owner, such as its logo or other trademark. In anti-counterfeiting terms, these solutions provide a clear distinguishing feature that sets apart branded products from their fake counterparts. The disadvantages, however, are similar to those with holograms. Given that these are passive technologies, there is a heavy reliance upon consumer ability to identify the special images (overt or semi-covert) and thereafter associating them with that particular brand. This kind of visual confirmation is an onerous task for most individuals, and becomes more so when counterfeited copies are introduced in the marketplace because of the greater confusion created in sorting through genuine from fake products. Although certain technologies in this sub-category can be more robust as a security feature in comparison to holograms, it is nevertheless true that duplication is extremely feasible by highly motivated counterfeiters. An example is the counterfeit Chinese 100 yuan bill shown in the figure, where a watermark of reasonable quality has actually been embedded in the fake currency (blue square)⁴³. There have also been instances of counterfeiting with OVI on fake currency⁴⁴.

The advantages of this group of passive technologies are that they are easily applied onto branded products, and especially documents. The result is an esthetically appealing end-result that can incorporate highly specific iconic images that are unique to the brand owner, such as its logo or other trademark. In anti-counterfeiting terms, these solutions provide a clear distinguishing feature that sets apart branded products from their fake counterparts. The disadvantages, however, are similar to those with holograms. Given that these are passive technologies, there is a heavy reliance upon consumer ability to identify the special images (overt or semi-covert) and thereafter associating them with that particular brand. This kind of visual confirmation is an onerous task for most individuals, and becomes more so when counterfeited copies are introduced in the marketplace because of the greater confusion created in sorting through genuine from fake products. Although certain technologies in this sub-category can be more robust as a security feature in comparison to holograms, it is nevertheless true that duplication is extremely feasible by highly motivated counterfeiters. An example is the counterfeit Chinese 100 yuan bill shown in the figure, where a watermark of reasonable quality has actually been embedded in the fake currency (blue square)⁴³. There have also been instances of counterfeiting with OVI on fake currency⁴⁴.

⁴⁰ 3M floats new anti-counterfeiting label. Article by G. Roumeliotis in In-Pharma, 2006. (<http://www.in-pharmatechnologist.com/Packaging/3M-floats-new-anti-counterfeiting-label>)

⁴¹ 3M Security Systems targets Indian pharma with range of counterfeit solutions. Article by N. Vijay in Pharmabiz, 2008. (<http://www.pharmabiz.com/article/detnews.asp?articleid=46168§ionid=2>)

⁴² Wikipedia entry. (http://en.wikipedia.org/wiki/Optically_Variable_Ink)

⁴³ Article in Asia Pundit, 2006. (<http://asiapundit.com/2006/05/16/fake-yuan/>)

⁴⁴ No Ordinary Counterfeiting. Article by S. Mihm in The New York Times, 2006. (<http://www.nytimes.com/2006/07/23/magazine/23counterfeit.html?pagewanted=1>)

c) Package modification

The final set of passive solutions concerns changes to product packaging or incorporating specialized packaging materials and formats. Package modification represents a low-tech solution, although the incorporation of new-age materials in the package can represent a fairly sophisticated approach⁴⁵. Many Indian brand owners in the past have tried to modify their packaging format with the reasoning that it forces the counterfeiter to spend large sums to follow suit. The assumption is that some may not bother to do so, or that there will be a delay during which the branded product is immune to the counterfeiting problem. A number of branded medicine packs, for example, have undergone packaging change to stay ahead of the counterfeiters, either by introduction of a new sleeve, a change in the colour and graphical design of the package, or simply altering the compositional layout.

The major advantage to adopting package modification as an anti-counterfeiting strategy is that it represents a minimalist approach in that no new technologies need to be evaluated or deployed. Many brand owners routinely alter their packaging formats in any case as a means of upgrading the appearance of their products in the retail setting. The disadvantage of this approach, however, is that it also represents a minimalist approach for the counterfeiter to keep pace and introduce fake products in an identically copied format. Counterfeiters have become increasingly sophisticated and can make use of advanced technologies to duplicate a package in as little as 12–18 months⁴⁶. The major investments often needed to modify retail packaging are therefore short-lived in terms of brand protection. Another disadvantage to package modification as an anti-counterfeiting strategy is that consumers must continually be made aware of the new format. The brand owner must therefore rely on customer memory and ability at identifying the correct package construction of a genuine branded product in the marketplace.

2. Active technologies

The second general category of anti-counterfeiting solutions is referred to as the *active technologies* because they all require an active process during the act of verification. The application of the various technologies in this category begins with the insertion or placement of a special marker or device, which is known as a taggant, into or upon the branded product. In some instances, the taggant can be placed on the package whereas in others, it can be incorporated directly into the product itself. In all cases, the subsequent act of authenticating the product requires a specialized device, reader, or scanner. Each type of taggant described in this section can only be detected by its own specific reader.

a) Electromagnetic taggants (RFID)

The most commonly used and widely known of the active technologies is radio frequency identification, or RFID. These taggants rely specifically on radio signals, which are emitted by an integrated chip or tag. The RFID tag itself can be placed anywhere within a package and in fact can be hidden because the emitted radio signals are able to penetrate through most materials. An RFID reader, which is a specialized instrument that detects the radio signals, can then be used to capture the information emitted by the tag. The information in turn is then transmitted to a software system that coordinates all aspects of the RFID operation.

The major use of RFID to date has been in terms of supply chain management. Although the technology has been around since the 1960s, recent advancements in chip technology and miniaturization have made RFID a viable choice in a number of such

⁴⁵ Wikipedia entry. (<http://en.wikipedia.org/wiki/Packaging>)

⁴⁶ *Anti-counterfeiting technology is not a silver bullet*. Article in PhRMA, 2008. (http://www.phrma.org/index.php?option=com_content&task=view&id=455&Itemid=120)

settings. The American retail giant Wal-Mart adopted RFID as a supply chain management tool, which in turn required the many suppliers who covet their relationship with Wal-Mart to implement RFID in their supply chain operations as well⁴⁷. There are a number of other RFID applications that have been adopted, including its use as a discrete information reservoir in passports, electronic toll collection on some European highways, aviation maintenance and overhaul, and asset management in health care settings.

The RFID technology, however, has not broken through in terms of its use as a pure anti-counterfeiting tool. To date, there is only one major example of RFID tags being applied at the product level, that being a pilot project on an expensive drug that has been a severe target of counterfeiting⁴⁸. Nevertheless, the RFID industry has undertaken major efforts to promote this technology as a valid anti-counterfeiting solution. Several large RFID players have established a presence in India, such as the 3M Corporation, which has announced a major initiative to expand RFID-based solutions for pharmaceutical products⁴⁹, as well as other global companies such as OAT Systems⁵⁰ and UPM Raflatac⁵¹. There are a number of Indian companies involved in RFID sales and support as well. The commercial interests of these indigenous RFID companies are represented by the RFID Association of India (RFIDAI).

The major advantages of RFID relate to its wireless nature. The tags do not require line-of-sight or any direct human intervention in order to capture the digital information. As a result, RFID tags can be hidden in packages so as to provide a greater level of security⁵². Furthermore, the tags can be read from a considerable distance, usually many metres, making it much easier to undertake roaming data capture⁵³. The tags can also be read rapidly in bulk, which is ideal for high-throughput supply chain tracking. And finally, RFID tags can contain significant amounts of information related to the product itself. In some cases, the reader can even write information directly to the tags, thereby making the RFID technology bi-directional in nature.

There are, however, a number of major disadvantages to the use of RFID as an anti-counterfeiting tool, which have been collectively responsible for its poor uptake in global

What is RFID?

RFID is a technology that allows identification of objects via a wireless communication system. The three components in a typical RFID system are the tag, reader, and software (also known as middleware).

An RFID tag is an integrated circuit mounted on a flexible substrate that can be adhesively applied to a product or container. The tag contains a unique tracking identifier, called an *electronic product code* (EPC), which is transmitted via radio waves through a built-in antenna. The specific frequency used by the newer generation of tags is in the range of 860 to 960 MHz (ultra-high frequency or UHF tags), whereas the older tags operate at 13.5 MHz (high frequency or HF tags).

An RFID reader captures the radio signal and provides network connectivity between tag data and the system software. The software supports a variety of functions that primarily include supply chain management tools but can also be used for product authentication purposes.

⁴⁷ *RFID is a hot topic*. Web article by Nutech Systems, 2005.

(http://www.nutechsystems.com/news_rfid.html)

⁴⁸ *Pfizer fights fake Viagra with RFID*. Article by A. Gilbert in CNET News, 2006.

(http://news.cnet.com/Pfizer-fights-fake-Viagra-with-RFID/2100-1012_3-6022485.html)

⁴⁹ Press Release reported in 3M News, 2008.

(http://multimedia.mmm.com/mws/mediawebserver_dyn?6666660Zjcf6lVs6EVs66Sok2C0rrrrQ-

⁵⁰ *OAT Systems to expand India Ops*. Article in The Financial Express, 2004.

(<http://www.financialexpress.com/news/OAT-Systems-To-Expand-India-Ops/115993/>)

⁵¹ Press Release by UPM Raflatac, 2007. (<http://w3.upm->

[kymmene.com/upm/internet/cms/upmcms.nsf/\\$all/56de6b6a94c9dd55c22573480034c8a0?OpenDocument&qm=menu,5,1,0&select=2007](http://w3.upm-kymmene.com/upm/internet/cms/upmcms.nsf/$all/56de6b6a94c9dd55c22573480034c8a0?OpenDocument&qm=menu,5,1,0&select=2007))

⁵² *The benefits of RFID technology*. Article by R. McGregor in Manufacturing & Logistics IT, 2007.

(<http://www.logisticsit.com/absolutenm/templates/article-critical.aspx?articleid=2883&zoneid=31>)

⁵³ *What is RFID*. Article in NextWave, 2007. (http://www.aimglobal.org/technologies/RFID/what_is_rfid.asp)

markets, and India in particular⁵⁴. The principal factors are cost, reliability, and privacy. The greatest burden to adopting RFID is a financial one. The cost of the tags can vary depending on volume, being typically in the range of 5–25 rupees per tag, which eliminates its use at the product level except for truly expensive brands⁵⁵. In addition to the tag cost, companies intending to adopt RFID must allocate very large sums for infrastructure development and implementation, making the capital investment requirement extremely burdensome⁵⁶. The second factor inhibiting RFID use is reliability, primarily due to reading errors. The problem with error rates comes down to physics. Radio waves are easily deflected or impeded by metals and liquids. It is therefore difficult to predict how radio signals will be bounced around inside a pallet or carton of goods. Estimates on error rates vary from study to study, but values in the range of 2.5%⁵⁷ to 25%⁵⁸ failure rate have been reported. And finally, major concerns have been expressed by privacy advocates who believe that RFID has the potential to capture personal information and thereby represents a larger problem for society. For example, if RFID should become widely adopted, then it is conceivable that a store owner can gather all sorts of information from any RFID tags that the consumer may have on them in addition to the products about to be purchased, such as a passport, any credit cards, garments being worn, other RFID-tagged retail products, and so on. This issue has raised considerable alarm among privacy advocates⁵⁹ and in some cases has led to public protests against the deployment of RFID⁶⁰. The concern is not just with the tags themselves but that the mere use of an RFID reader can allow someone to gather considerable personal information due to the wireless nature of the technology⁶¹.

b) Forensic taggants

The second group of active technologies encompasses a variety of different solutions, some of which are truly cutting-edge in nature. There is a large range of technologies that fall into this category, all of them requiring either laboratory testing or use of dedicated field test kits or specialized readers to prove product authenticity. It is for this reason that this group of technologies belongs in the category of *active taggants*. Forensic taggants have the common property of imparting a unique fingerprint to each product and for this reason, they provide an extremely strong forensic platform. The difference between the various technologies lies in the scientific methodology required for authentication.

Optical taggants

The simplest form of optical taggants use inks that are invisible under ordinary conditions but become visible with the use of a special filter or light source. An example is ultra-violet ink, which becomes visible when the product is illuminated by a UV source, causing the ink to radiate in the visible spectrum. The more robust optical taggants employ specific formulations of rare light-emitting chemicals that produce a complex spectral signature when illuminated by light of a specific colour and intensity⁶². The spectral

⁵⁴ *RFID: hype or reality?* Article by V. Aggarwal in Express Computer, 2008.

(<http://www.expresscomputeronline.com/20080908/market01.shtml>)

⁵⁵ *Will RFID Tags Click?* Article by S. Prasad in BusinessWeek, 2007.

(http://www.businessweek.com/globalbiz/content/may2007/gb20070531_589653.htm?chan=top+news_top+news+index_global+business)

⁵⁶ *Scoping Out The Real Costs of RFID.* Article by L. Shutzberg in InformationWeek, 2004.

(<http://www.informationweek.com/news/management/showArticle.jhtml?articleID=51201525>)

⁵⁷ *Are you reading me?* Article by K. Hunt in The Globe and Mail, 2007.

(<http://www.theglobeandmail.com/servlet/story/RTGAM.20070411.tgrifd0411/BNStory/GlobeTO/>)

⁵⁸ *The aviation supply chain has not rushed to embrace RFID.* Article by R. Mooman in Air Transport World, 2007.

(<http://www.atwonline.com/channels/safetySecurity/article.html?articleID=1968>)

⁵⁹ <http://www.angelfire.com/falcon/itfinal/RFIDdisadvantages.htm>

⁶⁰ *RFID Privacy Issues and News.* (<http://www.spychips.com/>)

⁶¹ *Passport card with chatty RFID chip draws privacy ire.* Article by J. Vijayan in Computerworld, 2008.

(<http://www.networkworld.com/news/2008/010908-passport-card-with-chatty-rfid.html>)

⁶² Source: DNA technologies (Australia) Pty. Ltd. website. (<http://www.dnatecaus.com/techOpt.htm>)

signature can be custom developed for each branded product and therefore the emitted light signal can be used for authentication purposes. The light signature itself is detected by a scanner-decoder that is customized for detecting the spectral signature in field or laboratory applications (see accompanying figure).

Chemical taggants

These technologies use a chemical marker that is applied either to a label or directly into the product itself. In terms of the latter, there exist a variety of inert compounds that can be added in trace quantities to edible products and medicines. In some cases, the detection process is more sophisticated because it involves spectrographic or chromatographic analysis in a laboratory setting. It is, however, possible to embed certain kinds of chemical taggants whose presence can be identified with a portable detector in the field⁶³. A variety of chemical products can be used as taggants, including inert resins, mild isotopes, and DNA fragments. The use of DNA fragments is a particularly intriguing method because it brings to bear cutting-edge molecular technology into the forensics arena⁶⁴. Either the product package itself or the ink used in the printing of a label can be laced with a unique DNA code that is virtually impossible to replicate. The absence of the DNA fingerprint provides significant forensic evidence to identify the product as being a counterfeit, whereas the presence of the DNA fragment provides confirmation of product authenticity.

Micro-particle taggants (nanotaggants)

Nanotaggants are microscopic particles containing coded information that can uniquely identify each branded product. The nanoscale markers are incorporated into the product or its packaging, which then exhibit distinctive properties that can be captured by way of a specialized reader. These unique properties provide forensic evidence for product authenticity and can also be used in terms of supply chain operations because each product is microscopically encoded⁶⁵. Nanotaggants have been successfully deployed in India to help contain fuel adulteration⁶⁶. The recent adoption of nanotaggants by the Indian company Bilcare Ltd. has made this technology available to the FMCG and pharmaceutical industries in terms of a packaging solution for addressing counterfeiting⁶⁷.

The advantage that the various types of forensic taggants offer is that they serve as extremely robust platforms for identifying fake products. These are generally high-technology offerings and therefore extremely secure against duplication. The disadvantages relate to the fact that all the different types of solutions are licensed technologies, and therefore limited to one source. As a result, these forensic technologies come at significant cost⁶⁸. And finally, the major restriction to these technologies is that they require either laboratory analysis or specialized readers. Consequently, none of these technologies provide consumer empowerment because an ordinary customer will not have any of these readers, which are generally quite expensive.

⁶³ *Anti-counterfeiting packaging*. Article in WorldPharma, 2008.

(http://www.worldpharmaceuticals.net/articles/wpf008_053_creoinc.htm)

⁶⁴ *DNA and consumer confidence*. Article by H. Breithaupt in EMBO Reports, 2003.

(<http://www.nature.com/embor/journal/v4/n3/full/embor782.html>)

⁶⁵ <http://www.nanoscienceworks.org/institutions/authentix-inc>

⁶⁶ *Nanotechnology helps contain fuel adulteration*. Article by S. Gunumurthi in MoneyControl.com, 2007.

(<http://www.moneycontrol.com/india/news/technology/nanotechnology-helps-contain-fuel-adulteration/21/44/288291>)

⁶⁷ *Bilcare plans big on anti-counterfeit technology*. Article in LiveMint.com, 2008.

(<http://www.livemint.com/2008/09/03154143/Bilcare-plans-big-on-anticoun.html>)

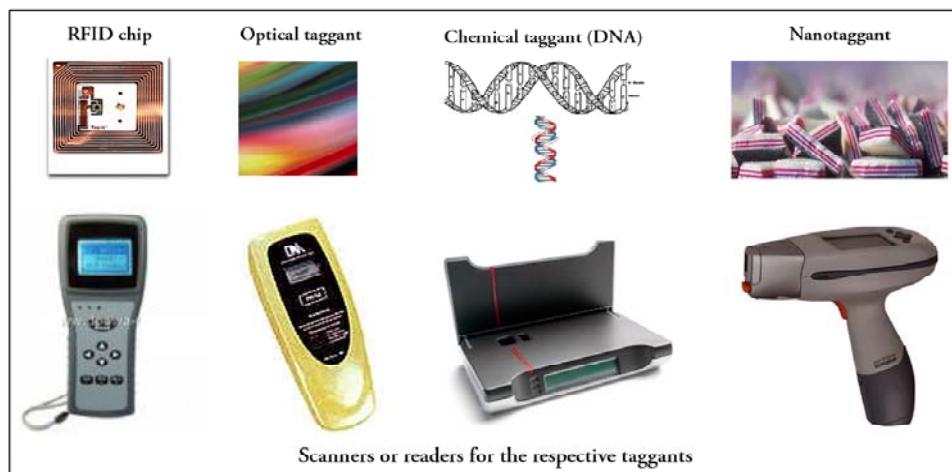
⁶⁸ *Anti-counterfeit Technologies for the Protection of Medicines*. Report of the World Health Organization.

(<http://www.who.int/impact/events/IMPACT-ACTechnologiesv3LIS.pdf>)

3. Mass encoding

The third general category of anti-counterfeiting solutions

encompasses those technologies that encode individual branded products in an overt digital manner. The digital information can appear on a product in terms of the universal linear barcode, or a new generation of 2D barcodes, or in human-readable form. The barcode technology is discussed first, followed by two methods of generating and processing the digital information. The core foundation of all of these technologies is that individually coded items can help combat counterfeiting because only genuine products will have a valid code. Furthermore, encoded products can be supported by enterprise software solutions that permit product tracking through the various nodes in the supply chain operation and therefore provide an electronic trace of the product's movement, which is becoming increasingly mandated by regulatory authorities.



Scanners or readers for the respective taggants

a) Barcode application

A barcode is an optical machine-readable representation of data whose technological origins can be traced back to the 1930s but adopted in mass retail settings only by the 1970s. Since then, this technology has developed into and maintained an overwhelming presence with regard to digital coding of consumer products⁶⁹. Virtually every item now purchased in a grocery store, department store, or mass merchandiser contains a barcode. The most commonly used barcodes are the linear or 1D (one-dimensional) pattern of lines. The coding system that is widely used, the so-called *Universal Product Code* (UPC), maps the data contained in the barcode to a standardized system of information representation. The data in a linear barcode can be captured by a wide variety of scanners, from high-throughput laser scanners used by many retail outfits to simple and cheap hand-held scanners. The digitized information is supported by back-end software for product identification purposes, supply chain management, asset tracking, inventory management, and various other functions that can be tailored to the needs of an individual client⁷⁰.

A new generation of barcodes has been recently developed that provide a 2-dimensional (2D) way of representing information. The biggest advantage to the 2D barcode technology is that much greater information can be encoded within a single barcode⁷¹. Furthermore, linear barcodes depend on links to a larger database whereas 2D barcodes can contain a mini-database themselves, and therefore encode much greater information on the product. The many benefits that 2D barcodes offer have led them to now become the default standard in many countries. The 2D barcode technology has also quickly become a rival to RFID as the most prominent track & trace technology. Although the US FDA has thus far not offered a preference, the European Federation of Pharmaceutical Industries and

⁶⁹ Wikipedia entry. (<http://en.wikipedia.org/wiki/Barcode>)

⁷⁰ Source: Barcoding Incorporation website. (<http://www.barcoding.com/>)

⁷¹ *How do 2D barcodes work?* Article in BBC News, 2006. (http://news.bbc.co.uk/2/hi/uk_news/magazine/5362740.stm)

Associations (EFPIA), a highly influential European trade group, has clearly come down on the side of 2D barcodes⁷². The results of a comprehensive study led them to announce their support in 2007⁷³ for a pan-European and industry-wide solution in which every medicinal product will contain a 2D barcode, "*instead of the less reliable and more expensive RFID*".

The advantages to using barcode application relate to the fact that this is a well-proven technology that has been in use for many decades and therefore enjoys substantial confidence in the retail marketplace. Furthermore, the cost is astonishingly low compared to all other technologies discussed thus far. For example, 2D barcodes offer similar functionalities to RFID at only a fraction of the cost. However, the real excitement in this field is being generated by the recent emergence of mobile decoders that allow consumers to actually use their mobile phones as a scanner for 2D barcodes. Some phone makers are already bundling their mobile phones with scanning software that decodes the 2D barcode image captured by the phone's built-in camera⁷⁴. This new development allows consumers to directly interact with the codes and obtain immediate validation, which is just one example of a host of other exciting possibilities⁷⁵. For example, all products sold in Japan are now tagged with 2D barcodes that allow consumers to validate their purchase and obtain important product information, such as the freshness of vegetables, the expiry date of medicines, and even to download memorable photos of a deceased person from the 2D barcode on a tombstone!^{76,77}. Furthermore, a 2D barcode standard has been recently developed by the airline industry for mobile phone check-in by passengers, something that has now been put into effect at certain airports^{78,79}. Given the fast pace of mobile technology development, it is highly likely that such consumer convenience and empowerment will soon be available in India.

What is a 2D barcode?

The 2D (two-dimensional) barcode is gradually replacing the traditional linear barcode that has been in use for decades. A linear barcode becomes wider as more data is encoded whereas 2D barcodes make use of the vertical dimension to pack in more data. A 2D barcode can store over 3,000 characters within a very small space as compared to just 20 characters in a linear barcode.

There are a number of different versions of 2D barcodes that have been developed, such as the Datamatrix and the QR formats. The Datamatrix format is becoming quite common on printed media due to the small size allowance and the fact that it can be read with up to 60% damage. The QR (Quick Response) code was developed in Japan as a fast decoding format that can also encode URLs, allowing readers to automatically launch websites after scanning. Both formats are public domain symbologies and therefore can be used free of licensing and royalties.



Datamatrix barcode



QR barcode

⁷² *Anti-Counterfeiting Strategies – Combating Fake Pharmaceuticals*. Publication by LeadDiscovery, 2007. (https://www.leaddiscovery.co.uk/reports/962/AntiCounterfeiting_Strategies_Combating_Fake_Pharmaceuticals)

⁷³ *Pharmaceutical industry backs 2-D bar code technology in the fight against counterfeits*. EFPIA Press Release, 2007. (http://www.pacmed.ca/Resources/EFPIA_PR_2007.pdf)

⁷⁴ *Samsung camera phones to come pre-loaded with Scanbuy's 2D barcode reader*. Article in Branding Unbound Blog, 2008. (<http://maverix.typepad.com/brandingunbound/2008/09/samsung-camera.html>)

⁷⁵ *Demonstrating the Cellphone Code Reader*. Article in The New York Times, 2007. (http://www.nytimes.com/2007/04/01/business/01codeside.html?_r=1&oref=slogin)

⁷⁶ *Japanese use cell phone QR bar code readers to check food safety*. Article by G. Nakada in Wireless Watch Japan, 2005. (<http://wirelesswatch.jp/2005/05/14/japanese-use-cell-phone-qr-bar-code-readers-to-check-food-safety/>)

⁷⁷ *2D barcode tombstone*. Article in Asiajin Blog, 2008. (<http://asiajin.com/blog/2008/03/13/2d-barcode-tombstone>)

⁷⁸ *Airlines announce bar code standard for cellphone check-ins*. Article by D. Melanson in Engadget, 2007. (<http://www.engadget.com/2007/10/16/airlines-announce-bar-code-standard-for-cellphone-check-ins/>)

⁷⁹ *Airlines adopt cell phone check-in for paperless boarding pass*. Article by I. King in L'Atelier, 2008. (<http://www.atelier-us.com/emerging-technologies/article/airlines-adopt-cell-phone-check-in-for-paperless-boarding-pass>)

The one drawback to all barcode technologies is that they were not originally developed for anti-counterfeiting applications, but rather as an inventory and supply chain management tool. As a result, a robust system of encoding products for authentication and brand protection via a universal standard was never put in place. This was not an oversight but reflected the fact that linear barcodes were simply limited in terms of their information capacity. The development of 2D barcodes, however, has now paved the way for their use as an anti-counterfeiting tool. In this regard, two new technologies have emerged that take advantage of the power of 2D barcodes and the rapid growth and sophistication of mobile telephony. These new technologies, which are referred to as *mass serialization* and *mass encryption*, are discussed in the next two subsections, respectively.

b) Digital mass serialization (DMS)

Digital mass serialization (henceforth referred to as DMS) is the process by which a unique number or code is assigned to each product sold in the retail marketplace. The code itself is similar in nature to serial numbers found on many products. It can be generated in a random, pseudo-random, or sequential manner. Once a batch of codes is generated, it is transferred to the brand owner so that they can be printed directly on the packages during the production process. Alternatively, the code itself can be pre-printed on a label and then affixed to the product in a manner similar to a hologram or security seal. DMS technologies can therefore be bundled with any of the other passive technologies to offer additional levels of security as well as ease of visual confirmation by the consumer.

The process by which DMS works is the following. Once the technology provider generates a code, it is entered into a database that can be used later at the verification stage⁸⁰. The database itself is managed and maintained either by the technology provider or the brand owner. The code is printed in human-readable form as well as a 2D barcode directly on the product or on a label. The codes themselves can be numeric, alphabetical, or alpha-numeric in nature. The consumer can visually read the printed script code whereas a barcode scanner can capture the 2D barcode. The emergence of mobile phones with barcode scanners now allows consumers to even use their mobile phones to directly read the 2D barcode. The pace at which mobile technology is exploding suggests that all consumers with a mobile phone will have this ability in the very near future⁸¹.

The authentication process involves matching the unique code on a product to those stored in the database. If the code is present in the database, then it is deemed to be authentic and so is the product. Several DMS providers in India have bundled this technology with their own SMS short-code number. Thus, all the consumer has to do to authenticate a product is to enter the code in the SMS field, send it to the short-code number, and then wait for the verification message, which usually arrives in a matter of seconds. The message will either provide confirmation of the product's authenticity or raise a flag if the code is not found in the database. The cumbersome act of manually entering the code in an SMS field can be bypassed with those phones containing barcode readers. In this case, the consumer simply takes a picture of the 2D barcode, which then automatically sends the code either as an SMS or through wireless internet to the DMS technology provider for verification. In some instances, brand owners may wish to incorporate toll-free SMS or call-in numbers to allow verification, thereby preventing customers from having to bear any mobile charges for the authentication process.

The major advancement that DMS technology brings to anti-counterfeiting efforts is that it directly empowers consumers to verify a branded product. As a result, a very large

⁸⁰ *RFID could be the future, but is it too long to wait?* Article by G. Metcalf in Pharmaceutical & Medical Packaging News, 2005. (<http://www.devicelink.com/pmpn/archive/05/01/015.html>)

⁸¹ *Mobile 2D barcodes: adding interactivity in a one-way world.* Article in InMoviMedia, 2008. (<http://www.inmovimedia.com/mobile-barcodes-2dcodes/>)

independent field force is recruited by brand owners to supplement their own direct vigilance of the marketplace. In terms of the latter, security officers can roam around with hand-held professional-grade barcode readers for rapid capture and verification of coded products. The twin aspects of consumer and professional vigilance provide immense deterrence because retailers who are involved in the sale of counterfeit goods will know that interdiction probability has suddenly become very high. Brand owners can implement a toll-free number, which consumers would use to tip off any failed verifications that can then be followed up by the company's own security officers or a private agency. A well-designed DMS system, however, will itself flag any failed authentication efforts and communicate this information to the brand owner, along with the date, time, place, and mobile number of the consumer who had made the verification attempt.

DMS offers a number of other important advantages that have led to immense acclaim by independent reviewers as well as regulatory agencies. Although these advantages are equally applicable to both the FMCG and pharmaceutical sectors, it is the latter where the urgency to implement DMS solutions has been especially vocal, leading a number of European countries to ensure that it is soon applied to their drug supply chain. A recent Frost & Sullivan report for the European pharmaceutical industry outlines the many advantages to using 2D barcodes and DMS as a supply chain management and anti-counterfeiting tool⁸². The European move follows on the heels of an earlier opinion by the US FDA to implement DMS, either by way of RFID or 2D barcoding. The 2004 FDA report on anti-counterfeiting was especially prescient in remarking that *'use of mass serialization to uniquely identify all drug products intended for use in the United States is the single most powerful tool available to secure the U.S. drug supply'*⁸³.

The major disadvantage to the DMS technology concerns the operational characteristics and security of the database containing the serial codes. It is well known that the larger a database becomes, the greater the time needed to find an individual item within it. Thus, a database containing hundreds of millions (or even billions) of codes for a major brand owner's annual production requirements becomes problematic in terms of database management and speed optimization. In such instances, the brand owner will have no choice but to adopt extremely high-end database software systems⁸⁴. Although these are extremely well-suited for the purpose, the annual licensing cost and employment of dedicated IT personnel with database systems experience can add significantly to the cost of the solution.

A related problem concerns database security. There are numerous examples in which even the most protected databases have been successfully hacked and information stolen⁸⁵. Although database files are usually maintained in an encrypted form, the fact that the databases of even major credit companies and defence agencies have been successfully intruded shows the limitations of file protection strategies⁸⁶. And finally, the security breach can be an internal one as well. Given the high level of mobility among IT employees in India, it is not inconceivable that a disgruntled database specialist can cause severe harm to a

⁸² *Mass Serialization in the European Pharmaceutical Industry*. White Paper by Frost & Sullivan, 2007. (<http://www.frost.com/prod/servlet/cio/140658996>)

⁸³ *Combating Counterfeit Drugs: A report of the Food and Drug Administration*, 2004. (http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html)

⁸⁴ *Addressing Pharmaceutical Counterfeiting and Fraud in the Real World*. White Paper by First OnDemand, 2007. (<http://expobadge.com/dldev/partners/file/LogiPharma%20White%20Paper%20draft6%20FINAL%20with%20Intro%206sept%2007%20V31Oct.pdf>)

⁸⁵ *The Web Hacking Incidents Database*. Annual Report of Web Application Security Consortium, 2007. (<http://www.webappsec.org/projects/whid/>)

⁸⁶ *Personal Data Security Breaches: Context and Incident Summaries*. Congressional Research Service Report, 2005. (http://digital.library.unt.edu/govdocs/crs/data/2005/upl-meta-crs-8258/RL33199_2005Dec16.pdf)

brand owner upon leaving the firm through malicious tampering or outright theft of the serial codes^{87,88}.

c) Digital mass encryption (DME)

Digital mass encryption (henceforth referred to as DME) is similar to DMS in all respects except for one major difference — the DME technology does not operate on a database system. As such, it offers all the advantages of DMS discussed in the last section but avoids its major drawbacks — requirement for database management, verification bottleneck at high volumes, and data security⁸⁹. DME can therefore be considered to be a more advanced and highly secure version of DMS. The DME solution is being separately described here because the core technology through which the codes are created and authenticated is fundamentally different from DMS.

Whereas serialized codes are generally created by random number generators, encrypted codes are produced by a cryptographic algorithm (see side box)⁹⁰. The DME algorithm is also responsible for the decoding process involved in the authentication step. Consequently, no database is ever created or required, either by the technology provider or the brand owner. The encrypted alphanumeric code is unique, unpredictable, and non-repetitive for eternity. The code can be used not only for authentication (anti-counterfeiting) purposes but also for hierarchical tracing in a complex supply chain operation. As such, DME is fully compliant with all regulatory standards, including the emerging *e-pedigree* requirements for pharmaceutical products in some countries⁹¹.

The DME technology was originally invented by the Norwegian company Kezzler AS for anti-counterfeiting and supply chain functions. The codes generated by their algorithm, which can be up to 16 digit alphanumeric in nature, are delivered to the brand owner and authenticated without any need whatsoever for either a database or any other type of storage and retrieval system⁹². The codes themselves do not carry or contain any product or logistical information; they serve simply as a transient link to such dynamic information that remains entirely under the control of the brand owner. An important aspect of this architecture is that the decoding process is not dependent on the volume of codes that were previously generated, but rather the computing time needed for running the authentication algorithm. Unlike the DMS technology, the speed of authentication in DME is

What is an encrypted code?

Cryptography is the practice and study of hiding information. In cryptography, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. In the DME context, the term “unreadable” means that a digital product identifier (the code) can be proven or disproven to be authentic only after having been decrypted by the original algorithm and the key by which it was generated.

The security of the coding system relies on safekeeping of the encryption keys, not the encryption algorithm, in accordance with Kerckhoff's principle and Shannon's maxim^a. DME makes it easy and uncomplicated to authenticate a product with an identifier, and at the same time makes it impossible to make a fake identifier.

^a http://www.knowledgerush.com/kr/encyclopedia/Shannon's_maxim/

⁸⁷ *City BPO accused of data theft*. Article in The Times of India, 2008.

(http://timesofindia.indiatimes.com/Ahmedabad/City_BPO_accused_of_data_theft/articleshow/3081539.cms)

⁸⁸ *Arrest made over HSBC Indian call centre theft*. Article by A. McCue, 2006.

(http://www.silicon.com/financialservices/0_3800010322_39159991_00.htm)

⁸⁹ *Countering Counterfeits*. Pharmabiz Chronicle Special, Interphex India 2007, Mumbai.

(<http://www.pharmabiz.com/article/detnews.asp?articleid=40641§ionid=50>)

⁹⁰ Wikipedia entry: (http://en.wikipedia.org/wiki/Key_size)

⁹¹ *Impact of Counterfeit Drugs on Healthcare Combating Alternatives: An overview*. Article by R. Hemalatha, 2007.

(<http://www.pharmainfo.net/reviews/impact-counterfeit-drugs-healthcare-combating-alternatives-overview>)

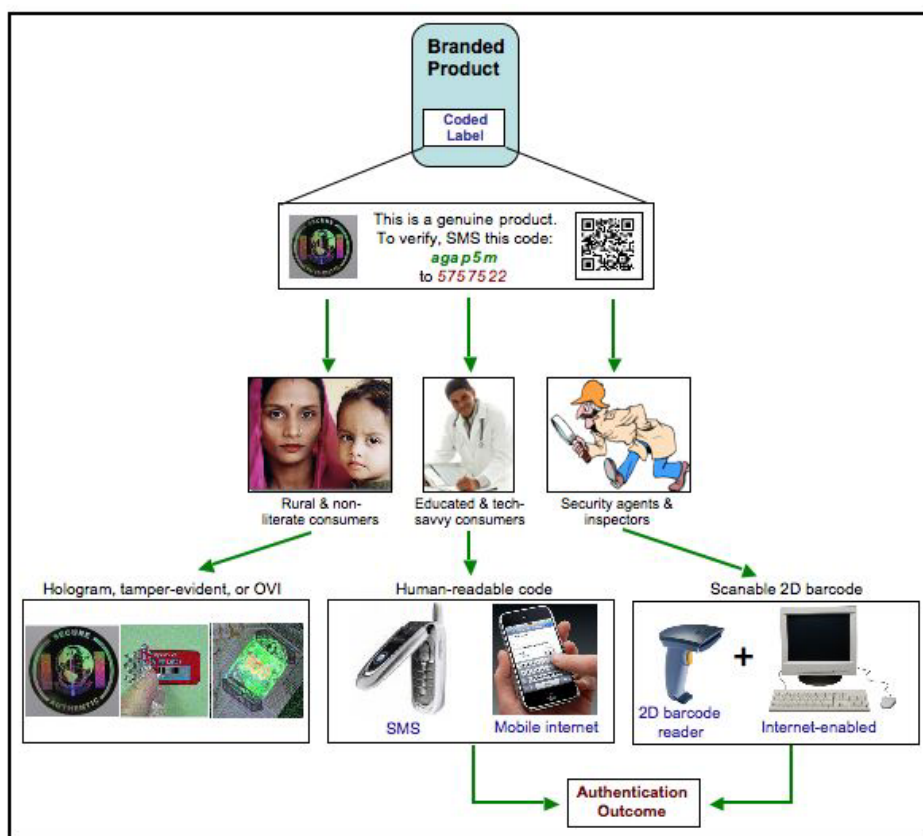
⁹² *Theory and Principles of Digital Product Security and Secure Trans and Trace*. White paper by Kezzler, 2008.

(https://kezzlercoding.com/mediawiki/index.php/Theory_and_Principles_of_Digital_Product_Security_and_Secure_Track_and_Trace)

in fact the same whether one thousand or one billion codes were delivered to a particular brand owner. As a result, DME is an extremely high-throughput security system that is ideally suited for very large product volumes.

The operational aspects of the DME technology are otherwise similar to those of DMS. The code itself is typically valid for only one authentication. Multiple authentications attempts of the same code will raise an alert. This allowance denies the ability of a counterfeiter to copy one valid code and apply it onto many fake products as a means of trying to bypass the DME system. Multiple failed authentications of the same code will raise a flag and when confirmation is made that a particular code has been duplicated on fake products, *that* code itself serves as a tag by which the fake products can be identified. In such instances, consumers are directly warned that the product is fake and that they should report this case along with other pertinent information to the brand owner (or its appointed security agency). The ability to actually identify fake products in the marketplace and directly warn consumers is a twist of fate that was likely unbeknownst to the counterfeiter.

The recent decision by Kezzler AS to enter into India highlights both the market potential as well as the need for a cost-effective and highly robust solution to combating FMCG and pharmaceutical counterfeiting. The move to introduce DME in India has been met with significant interest by the mainstream media^{93,94}. Furthermore, a recent review of various technologies by EIPR Inc., India's largest private investigation agency specializing in anti-counterfeiting and IP fraud, led them to assert DME as "the ideal anti-counterfeiting technology" for India because of features such as its low cost, forensic applicability, and consumer empowerment⁹⁵. It should be noted that EIPR and Kezzler have forged a strategic partnership wherein the DME technology would help empower EIPR's security force in its field investigations.



⁹³ CNBC News Report, 2007. (http://www.in.com/active18/watchnow/watchvideo_mc.php?autono=294185)

⁹⁴ CNN-IBN News Report, 2008. (<http://www.ibnlive.com/videos/72391/sms-to-know-if-the-product-you-are-buying-is-fake.html>)

⁹⁵ EIPR & Kezzler join to combat counterfeiting in India. Article in Moneycontrol.com, 2008. (http://news.moneycontrol.com/mccode/news/article/news_article.php?autono=352500)

As with DMS, the DME technology can be bundled with various passive technologies to provide greater consumer outreach, security, and esthetics. The accompanying figure provides an example of how this can be attained⁹⁶. In this scenario, the branded product contains a label with the DME code and instructions for its use⁹⁷. The label also contains a 2D barcode and a hologram. There are various other options that a brand owner can opt for, such as use of OVI written text, hidden images, a tamper-evident label, etc. The combination of all three features — DME, hologram, 2D barcode — provides considerable breadth for use as an anti-counterfeiting solution. For example, the presence of the holographic image, which may be the brand owner's logo, can be used as a means of passive verification for mass use, especially in rural areas or by individuals with limited literacy. The DME code, on the other hand, can be used by anyone with a mobile phone to authenticate the product at the point of sale, either through SMS or by way of mobile internet for those phones enabled with a barcode reader (e.g., iPhone and various models of Nokia, Samsung, and Sony Ericsson phones). And finally, the 2D barcode can be used by security agents employed by the brand owner to undertake large-scale random checks of their products in the marketplace. There is a large range of 2D barcode readers, some that are Bluetooth enabled, which would permit an agent to simply capture the coded information and either immediately verify at the retail outlet using mobile technology or to undertake later analysis in batch mode through an internet-enabled computer.

The various advantages of the DME technology have been previously discussed. The disadvantage to DME is that at present, the only provider of this technology in India is Kezzler AS. However, the price point that Kezzler has arrived at for the Indian market is substantially discounted and scaled for volume, which makes it extremely appealing for brand owners with large annual production volumes where the cost per code can be merely a few paisa (or even fractions of a paisa for extremely high volumes)⁹⁸. The flipside, however, is that brand owners with small annual volumes of a low-cost product will likely be frozen out of the DME technology because the price discount in this case is not as lucrative.

⁹⁶ This figure has been adapted from a similar one contained in Reference # 87, with permission.

⁹⁷ The sample DME code in this figure is active and can be verified by SMS to the number given, courtesy of Kezzler AS.

⁹⁸ Based on pricing information provided by Kezzler's India agent, PAC Med Biotech Pvt. Ltd.

E. Technology Comparisons

The discussion in Section D of this manual describing the three major categories of anti-counterfeiting solutions now paves the way for a head-to-head comparison to determine which technologies are most suitable. As a quick reminder, the passive technologies are based on mere visual inspection of a product and include holographic labels and various types of security seals, as well as overt and semi-covert imaging techniques. The active technologies encompass RFID and various types of forensic taggants (optical, chemical, microscopic). And finally, the third category, which is called mass encoding, primarily includes DMS and DME. Barcodes are not considered in the comparisons below because they only serve as data carriers of DMS or DME codes in the anti-counterfeiting context.

These three categories of anti-counterfeiting technologies are now compared and contrasted in relation to the five Golden Qualities that were described in Section B. The accompanying figure summarizes how each technological category fares against the five Golden Qualities. This figure should be referenced during the course of the ensuing discussions.

Golden Quality	Passive	Active	DMS/DME
Consumer empowerment			
Technology can be implemented at product level	✓	✓	✓
Consumer can use technology to verify product authenticity at point of sale	?	x	✓
Technology permits robust identification of fake products by consumer	x	x	✓
Overall grade	Fail	Fail	Pass
Cost and value			
Technology is difficult to duplicate	?	✓	✓
Low capital investment	✓	x	✓
Low running cost	✓	x	✓
Overall grade	Pass	Fail	Pass
Forensics and interdiction			
Technology serves as a robust forensic tool	x	✓	✓
Strong interdiction & prosecution abilities	x	✓	✓
Overall grade	Fail	Pass	Pass
Simplicity and adaptability			
Technology is easy to implement by brand owner at factory level	✓	x	✓
Technology is highly adaptable to evolving and unforeseen changes in the brand	✓	✓	✓
Overall grade	Pass	Mixed	Pass
Value-added features			
Technology permits consumer outreach and promotional campaigns	x	x	✓
Obtain sales information & market intelligence	x	x	✓
Technology allows supply chain management (Track & Trace capabilities)	x	✓	✓
Meets regulatory standards (e-pedigree)	x	✓	✓
Overall grade	Fail	Mixed	Pass

Consumer empowerment (Golden Quality #1)

The good news is that the technologies represented in all three categories can be implemented at the individual product level. The situation changes considerably, however, when one assesses the ability of an ordinary consumer to use the technology for authenticating a branded product. Passive technologies allow a consumer to determine that a hologram or some other visible feature is present. The challenge is to know what to look for and to be savvy enough to interpret a hidden image or be able to turn a product just enough to notice the changing colors in OVI print. This requirement becomes particularly problematic when a counterfeiter introduces a fake version of one of the passive technologies, such as a hologram. It is virtually impossible for ordinary consumers to identify a true hologram from a fake one. Thus, passive technologies when used alone do not sufficiently empower consumers in terms of product authentication.

Active technologies are also poor in terms of consumer empowerment because customers do not carry around the special readers that are needed for verification. Thus, even if a branded product is protected with any of the sophisticated offerings in this category, the technology would simply be impenetrable to consumers. As a result, none of the positive aspects associated with consumer empowerment are made available to the brand owner when implementing an active technology.

The only technologies to attain a passing grade in terms of this core Golden Quality are the DMS and DME solutions. When used as a stand-alone feature, the DMS and DME codes can be verified via SMS on a mobile phone, which currently has a market of close to 300 million in India⁹⁹. When bundled with any of the passive technologies, both DMS and DME provide much greater coverage in terms of product protection on a mass scale. However, it is the codes that clearly provide stringency in protection. As an example, the biggest counterfeiting bust in history involved Windows Vista software, with a value estimated at more than five hundred million dollars. Fake software disks contained holograms that were near perfect replicas of those belonging to the branded version. It was the serialized code that is part of the Microsoft package, however, submitted by customers that alerted the brand owner and helped trace the source to a criminal syndicate in Southern China¹⁰⁰.

To summarize, only DMS and DME solutions pass the consumer empowerment requirement that forms the first Golden Quality in an anti-counterfeiting technology.

Cost and Value (Golden Quality #2)

A core aspect of the value proposition relates to difficulty in duplication. The more robust the technology, the harder it is to duplicate and therefore provides a longer lifetime of service to the brand owner. As noted above, holograms are notoriously easy to replicate. Some of the other passive technologies, however, can be more robust but are nevertheless vulnerable in their own way. Both the active technologies and mass encoding, however, are superior in this regard. All the active technologies are sufficiently sophisticated so as to make duplication virtually impossible. Similarly, codes generated by DMS and DME systems are difficult to guess; in fact, the chances of winning a lottery would be far greater. The only caveat is that the database requirement of DMS makes it vulnerable to hacking, which is not a concern with DME. A lost bank of codes can be potentially devastating to a brand owner, not only in terms of a security breach but also as a public relations matter.

In terms of cost, the active technologies suffer heavily due to both the capital investment needed to implement these systems as well as the residual cost on a per product basis. Furthermore, readers or scanners can be quite costly, with some being extremely advanced devices that are only available from the technology provider. Although RFID scanners have now come down in cost, the RFID tags themselves continue to pose a major concern. Several high-profile pilot studies have failed to make a convincing case for adopting this technology, primarily due to cost and implementation concerns¹⁰¹. Although RFID has shown its suitability as a high-volume supply chain management tool, it is not an appropriate stand-alone anti-counterfeiting solution.

The two technology categories that generally require low capital investment and running cost are passive technologies and mass encoding. There are, however, subtleties that should be considered. Passive technologies involving label application are generally faster to implement than those involving direct etching on a package in the production line. Similarly, DMS and DME code printing directly on the package requires ink jet printers that are of sufficient resolution to allow veridical scripted code and 2D barcode printing. Here again, label application offers a simpler start-up solution to immediately initiate brand protection, though in the long run direct printing will be more cost effective and easily make up for any needed investment in new printers. Regardless of the option chosen, it is important for brand owners to undertake a pilot study to fully understand implementation

⁹⁹ *India adds 9.22 million mobile phone connections in July.* Article by J. Ribeiro in MIS Asia, 2008. (<http://mis-asia.com/news/articles/india-adds-9.22-million-mobile-phone-connections-in-july>)

¹⁰⁰ *Sting! The biggest software counterfeiting bust in history.* Article by A. Kochis in Windows Vista News, 2007. (<http://windowsvistablog.com/blogs/windowsvista/archive/2007/07/24/the-biggest-software-counterfeiting-bust-in-history.aspx>)

¹⁰¹ *GSK plan to beat drug counterfeiters may be scrapped.* Article by R. Pagnamenta in Times Online, 2007. (http://business.timesonline.co.uk/tol/business/industry_sectors/health/article2324186.ece)

requirements and discover any inherent pitfalls that may un hinge a major roll-out when that technology is fully adopted.

To summarize, active technologies fail in terms of the second Golden Quality whereas both passive and mass encoding technologies pass it.

Forensics and interdiction (Golden Quality #3)

Passive technologies are entirely inadequate in terms of forensic applicability by virtue of their ease of duplication and the generality of their intrinsic features. For example, a well-replicated fake hologram can certainly be shown to be fake, but only after careful scrutiny by an industry expert. The same holds true for overt and hidden image applications. Watermarks, for example, are notoriously easy to duplicate and fake versions have been found in counterfeit currency notes. This lack of a strong forensic platform also means that interdiction (and eventual prosecution) is difficult with passive technologies.

Both active technologies and DMS/DME represent extremely strong forensic platforms. The sophisticated nature of active technologies and the specificity of detection empower security agents to make a forensic determination on the spot in most cases. The only caveat relates to those active technologies that require laboratory analysis for confirmation. Although forensic use remains strong in this case, the lack of immediacy at the point of sale mitigates interdiction capabilities. Mass encoding also offers strong forensic applicability. If a branded product is supposed to have a code but does not, then it is a fake product. If many products in a shop have the same code, then they are all fakes. If a code is present, but does not pass the authentication step, then it is a fake. Thus, a printed code, when present, is either valid or not. Brand owners must ensure that any mass encoding solution does not invalidate a code when authenticated during random inspection by a security agent. The DME platform allows brand owners to register the mobile phones of their security agent so that market vigilance by such individuals will not invalidate the code, which have a one-time limit on public authentication.

To summarize, both active technologies and mass encoding pass in terms of the third Golden Quality whereas passive technologies do not.

Simplicity and adaptability (Golden Quality #4)

Passive technologies and mass encoding have the advantage of being less intrusive in terms of implementation in the production line. In most cases, both technologies will require label application, which can be undertaken in an automated or semi-automated manner. Label application is common in most industries and therefore a variety of options are at the disposal of the brand owner. Active technologies, however, require greater sophistication in terms of implementation. Although RFID tags can be easily applied, the infrastructure that is required to fully implement a robust RFID solution is quite involved. Similarly, various forensic taggants each have their own specialized requirements in terms of application. Some can be embedded into the product itself whereas others are applied on the package. In general, these technologies necessitate specialized solutions that can be fairly intrusive for most industrial applications. The technologies in all three categories are fairly adaptable in that new variants can be introduced after they have been implemented. Although there may be subtle differences between individual exemplars within a given category, those differences are not sufficient to warrant overt concerns. Technological adaptability allows brand owners to modify the brand protection solution to changes that take place in terms of new package design, brand evolution, or other externally imposed conditions.

To summarize, both passive technologies and mass encoding pass in terms of the fourth Golden Quality whereas active technologies have a mixed outcome, driven primarily by concerns regarding implementation.

Value-added features (Golden Quality #5)

There are a number of different value-added features that can be incorporated into any anti-counterfeiting solution. The two features that appeared most important to brand owners during the preparation of this manual were added marketing uses of the technology and applications in terms of supply chain management. The latter is a core feature of many technologies because one path to brand protection is having a secure supply chain. Although it is now clear that this alone does not protect a brand, due to infiltration by third parties at various points such as the retail level, the oft-expressed opinion is that a technology that provides a distribution management tool would represent an important supplemental feature. A somewhat different wish was expressed by brand owners who wanted to use the consumer empowerment feature in an anti-counterfeiting technology as a bi-directional communication tool, and thereby allow it to serve as an advanced new portal for consumer outreach and product promotion.

How do the various anti-counterfeiting technologies fare in these two regards? The clear loser in terms of both value-added features is the passive technologies. All offerings in this category are merely visual tags, emblems, or images. As such, there is no communication portal and hence no possibility for use as a marketing tool. Furthermore, passive technologies do not provide any supply chain management functions because there is no scope for scanning the product at any point in the distribution process.

Most of the active technologies, however, provide this feature and associated software to track products through the supply chain. Furthermore, many technologies are compliant with regulatory frameworks that demand an e-pedigree. The major drawback to active solutions, however, is that they cannot be used as a marketing and promotional tool because there is no consumer interaction with these technologies.

The mass encoding solutions encompassing DMS and DME are excellent in terms of both value-added features. The 2D barcodes, as carriers of digital information, can fully support a comprehensive supply chain operation and maintain regulatory compliance. The tracking and tracing function in this regard can be visualized as being similar to a courier package that moves from a source to a destination. At each node in the path, the package is scanned and its precise location is available in real time. The same scenario is present in tracking and tracing of branded products throughout the supply chain. The only cautionary note, however, is that brand owners must ensure that supporting software systems are fully integrated with the technology and are compliant with regulatory requirements, such as generating e-pedigrees. An important feature to look for is whether the technology provider has designed the software itself or whether it is offering a third-party solution. The latter should be avoided. Some DMS vendors only offer an SMS-based authentication solution and do not provide either 2D barcoding or supply chain management support. It is not in the brand owner's long-term interests to invest in mass encoding technology whose functionality is limited to only product authentication.

The mass encoding technologies also provide brand owners with significant added value in term of marketing use. The mobile phone is essentially the reader of DMS and DME codes, either by means of manual entry or automated scanning with the phone's camera. Regardless of the code entry method, a bounce-back message sent by the brand owner can contain a considerable amount of information in addition to validating the product. Some examples of additional content in a bounce-back message include brand information, product updates, MRP, promotional messages, details on events being sponsored by the

brand owner, and advance information on any new product introductions. The message may also contain expiry date and usage warnings, which are especially important for pharmaceutical brands. Recalls, when necessary, can also be communicated via SMS messaging because the brand owner has the mobile phone contacts of all users who have authenticated the product. And finally, those brand owners that have a creative marketing department can use this tool to further promote their products by way of loyalty programs, contests, and lotteries to boost market share. As a result, the twin combinations of a software-based anti-counterfeiting solution in tandem with the power of mobile communication have created considerable excitement with regard to DMS and DME.

To summarize, passive technologies do not offer sufficient value-added features to pass in terms of the fifth and final Golden Quality. Active technologies obtain a mixed grade, being excellent in terms of distribution support but extremely poor as a consumer outreach tool. Mass encoding technologies are superior in both respects because of their inherent bi-directional nature of communication and breadth in consumer outreach.

Overall summary (technology-based)

	Consumer empowerment	Cost & Value	Forensics & Interdiction	Simplicity & Adaptability	Value-Added Features
Passive Technologies	Fail	Pass	Fail	Pass	Fail
Active Technologies	Fail	Fail	Pass	Mixed	Mixed
Mass Encoding	Pass	Pass	Pass	Pass	Pass

Overall results of the analysis undertaken in this section are summarized in the accompanying figure in terms of how each technology performs under the various criteria that were considered. Passive technologies receive a passing grade in terms of cost & value (Golden Quality #2) and simplicity & adaptability (#4). They fail in terms of consumer empowerment (#1), forensics & interdiction (#3) and value-added features (#5).

Active technologies receive a passing grade in terms of forensics & interdiction (#3) but produce a mixed report in terms of simplicity & adaptability (#4) and value-added features (#5). They fail in terms of consumer empowerment (#1) and cost & value (#2).

Mass encoding technologies (DMS & DME) receive a passing grade in terms of all five Golden Qualities.

F. Choosing the Right Technology — Recommendations for Indian Industry

For most brand owners, the path to choosing the right technology is a complex undertaking that requires sound judgment in adopting a solution with the best overall characteristics as well as one that is ideally suited for the specific needs of that company. The preceding two sections have described the various anti-counterfeiting technologies and compared them with regard to the fundamental qualities that they should possess, expressed in this manual as Golden Qualities. The objective of this section is to help brand owners determine which technologies should be evaluated in the first place, given the volume and price point of their branded product. This section concludes with an outline of the key steps involved in adopting the right anti-counterfeiting technology.

The volume-value matrix

The starting point for finding the right brand protection solution is to first understand which technologies are suitable for a particular product in the context of two important parameters — its annual production volume and the product’s MRP. Once that delineation is made, the brand owner can then evaluate offerings within each suitable technology category by taking into account the features described in this manual along with perspectives offered in terms of how they fare against the five Golden Qualities.

		Value (MRP per protected unit)			
		Ultra-low (< 20 Rs)	Low (20 - 100 Rs)	Medium (100 - 500 Rs)	High (>500 Rs)
Volume (annual sales in units)	Ultra-low (< 1 m)	Passive DMS	Passive DMS	Active DMS	Active DMS DME
	Low (1 - 10 m)	Passive DMS	Passive DMS DME	Active DMS DME	Active DMS DME
	Medium (10 - 100 m)	Passive DME	Passive DME	Active DME	Active DME
	High (>100 m)	Passive DME	Passive DME	Active DME	Active DME

The ideal technology category (Passive, Active, or Mass Encoding) can be determined from the accompanying table, which is henceforth referred to as the *volume-value* matrix (VVM). The annual production volume in saleable units is represented in a row-wise manner and categorized in terms of ultra-low (< 1 million), low (1-10 million), medium (10-100 million), and high (>100 million). The MRP of the product is shown in columnar fashion and placed in similar categories, i.e., ultra-low (< 20 Rs), low (20-100 Rs), medium (100-500 Rs), and high (>500 Rs).

Each cell in the VVM shows the technology categories that are optimally suited for that particular intersection of volume and value (price). The two mass encoding technologies — DMS and DME — are separately represented in this matrix because of their inherent qualities that are separable in terms of volume optimization.

For some companies, this matrix will be referenced with regard to one particular brand, or a small number of brands, that are being targeted by counterfeiters. For other companies, the entire product portfolio may be considered for protection, in which case the value indexes may span several columns of the VVM.

The discussion that follows is divided into a technological one, in which the justification for placement of the different anti-counterfeiting solutions in the matrix is given, followed by a discussion on use of the VVM from the point of view of the brand owner.

Technology perspective

The principal factor that differentiates passive and active technologies in the VVM is the price of the product under consideration. For those branded products that are of ultra-low and low value, the optimal solution may be any of the passive technologies. On the other hand, if the product's MRP places it in the two higher categories, then the passive technologies become less suitable and a transition occurs toward consideration of the active technologies. The mass encoding technologies are applicable across all price points, as shown in the VVM.

While the horizontal meridian serves as the differentiator for the passive *versus* active technologies, the vertical meridian delineates the DMS *versus* DME technologies. DMS is suitable at low annual volumes where the concern with database management is less acute. At high volumes, a significant decline in the price of the DME technology along with the absence of a database makes this the preferred choice.

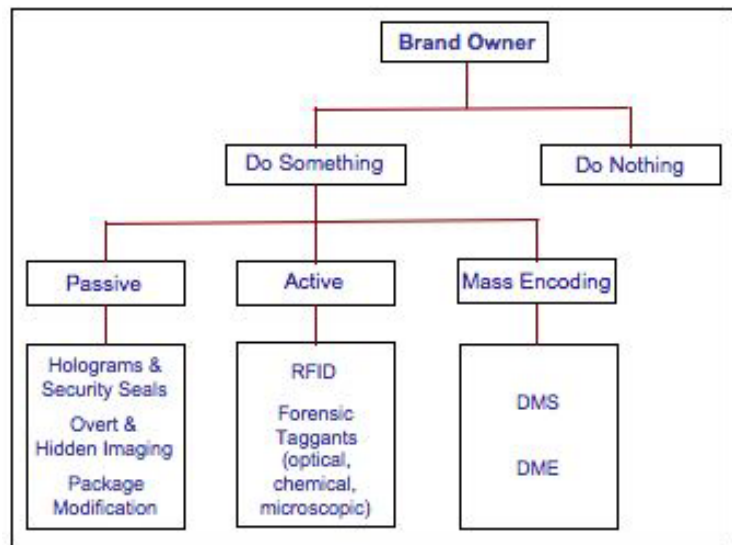
Industry perspective

Regardless of how great a particular brand protection solution is, the first and foremost consideration for corporate executives is to ensure that the technology is cost-effective. Thus, the primary criterion applied in creating the VVM was the cost of the technology. The individual cells in this matrix have been filled with those technological categories likely to have vendors whose solutions will adhere to the 1% rule — i.e., that the cost of an anti-counterfeiting technology should be in the range of 0.1 – 1.0% of the product's MRP and should not exceed the upper limit.

Branded products whose MRP falls in the ultra-low and low cost categories have essentially two choices — passive technologies and mass encoding. If annual product volume is also in the ultra-low and low domains, then the preferred mass encoding solution should be DMS. If, on the other hand, annual production volume reaches medium and high domains, then DME joins passive technologies as the solution that should be considered. Although DMS can still be explored in these cases, high code volumes are better suited for DME because it does not require database management. Furthermore, the price of DME is scaled to volume and therefore it is likely to be more cost-effective at these high volumes for ultra-low and low cost brands.

The situation becomes somewhat more complicated when the product price reaches the medium and high value domains. As evident in the VVM, passive technologies now give way to the active technologies because they are more of a niche solution and therefore better suited for higher priced products. Furthermore, consumers are likely to demand a more sophisticated solution than the low-cost passive technologies for such brands. At ultra-low volumes, DMS remains the preferred mass encoding solution. However, DME begins to show greater preference at lower volumes in these higher price categories and should be considered.

An interesting situation arises with power brands that have ultra-high annual production volumes, i.e., exceeding 500 million saleable products. The question naturally arises as to which solution is optimal for these brands. In such cases, both the active and DME technologies should be considered. However, the cost of DME will likely remain an attractive feature. Furthermore, major brand owners will benefit from the consumer empowerment features of DME and the various outreach and value-added marketing opportunities that are available, which is not so with any of the active technologies¹⁰²¹⁰³.



The next steps

Brand owners currently targeted by counterfeiters are faced with three levels of decision making. The first level in the decision tree involves making a strategic choice of whether to do something or nothing about counterfeiting. Senior management of a company must decide whether to adopt a *laissez-faire* attitude or to take a proactive approach. The multiple factors that guide these two outcomes were explored in detail in Section B earlier.

In the event that a decision is made to proceed with a proactive approach, then the next level is reached — determining which of the three general categories of anti-counterfeiting solutions is best suited for their brands. The volume-value matrix provides the starting point for making this decision. A careful survey of the properties of each category within the applicable VVM cell should then be made in terms of the fundamental qualities that are being sought in the solution. Section C of this manual presented five so-called Golden Qualities that were meant to serve as a guide for purposes of evaluation.

The next step for the brand owner is to determine which of the Golden Qualities are truly important. For example, some companies may covet a sophisticated forensic solution and not be concerned with consumer empowerment because they have a strong field force of security agents that keeps vigilance over the marketplace. Other brand owners, however, may value the consumer empowerment features of mass encoding technologies and conclude that the opportunity to boost market share through an advanced new portal is a tantalizing feature. Regardless of the factors operative in any given company, a careful comparison should be made across multiple technology offerings. Section D of this manual provided a comprehensive description of the various anti-counterfeiting solutions and Section E provided a head-to-head comparison between them. The outcome of this evaluation should lead the brand owner to determine which particular category — passive, active, or mass encoding — is the most suitable for their purposes.

The third level in the decision tree is to evaluate vendors within that technology category to ensure that the solution is both cost-effective and meets the needs of the brand

¹⁰² Roche implements 'mass serialization' anti-counterfeit technology. Article by P. Reddy in SpicyIP, 2008. (<http://spicyipindia.blogspot.com/2008/10/roche-implements-mass-serialization.html>)

¹⁰³ Firms adopt new ways to fight back. Article by L. Joseph in Wall Street Journal Online, 2008. (<http://www.livemint.com/2008/11/02204451/Firms-adopt-new-ways-to-fight.html>)

owner. Technology vendors must be able to make a convincing case in terms of both parameters. One approach to obtaining greater confidence and assurance is to undertake a pilot study, as discussed earlier in this manual. All technology providers should be willing to be cooperative in this regard and a reasonable price should be negotiated that would ensure fairness and parity on the part of the potential supplier and buyer.

The only remaining matter is to identify the actual vendors of the various brand protection technologies. The appendix of this manual (Section G) provides the names of over fifty global technology providers, with over twenty that have an operational presence in India, which are identified in bold along with their contact information.

Use of this manual

The objective of this manual was to assemble current information on anti-counterfeiting technologies and classify them into categories that would simplify comparison, as opposed to the immensely cumbersome process of separately evaluating each of the many brand-protection solutions. This manual also aimed to serve two purposes — first, to provide a comprehensive and objective appraisal of currently-available anti-counterfeiting technologies, and second, as an advocacy channel in terms of how to proceed in identifying the right technology, the features to look for, and the pitfalls to avoid. As such, this document should serve as a core reference manual for Indian industries currently grappling with the menace of fraud and counterfeiting. It is expected that this document will be updated in the future as warranted and the contents revised in light of emerging new trends and opportunities for the Indian brand owner.

G. Appendix — Selective List of Technology Companies

A list of anti-counterfeiting and brand security companies along with the categories to which their technology belongs (Passive, Active, or Mass Encoding). Indian companies or foreign companies with an Indian presence are shown in bold type in the first column ('Company') along with the Indian contact information taken from their website.

Technology Provider			Technology Platform		
Company	Website	Indian Contact	Passive	Active	Mass Encoding
3M	http://solutions.3m.com/wps/portal/3M/en_IN/Worlwide/WW	3M India; +91 80 2223 1414	Security seals; overt & hidden imaging	RFID	
Acucote Inc.	www.acucote.com		Security seals; overt imaging		
Alcan Packaging	www.globalpharma.alcanpackaging.com		Overt imaging; specialized packaging		
AlpVision	www.alpvision.com			Optical taggant	
AMCO Plastic Materials	www.amco.ws/anticounterfeiting			Chemical taggant; nanotaggant	
Angstrom Technologies	www.angstromtechnologies.com			Optical taggant	
Applied DNA Sciences	www.adnas.com			Chemical taggant	
ARmark™ Authentication Technologies	www.rmark.org			Chemical taggant; nanotaggant	
ASD Inc.	www.asdi.com	Indian Agent: Electrotek International Inc.; +91 44 2499 5816; seismo@electrotekintl.com		Chemical taggant	
Authentix	www.authentix.com	Business Development Office, New Delhi; +91 11 4140 3908		Chemical taggant; nanotaggant	DMS
Bilcare	www.bilcare.com	Bilcare Ltd.; direct-in@bilcare.com	Package modification	Nanotaggant	
BP Labels	www.bplabels.co.uk		Security seals; overt imaging		
Brady Corporation	www.bradycorp.com	Brady Company India Pvt. Ltd., +91 80 6658 2900; anitha_p@bradycorp.com	Security seals; overt & hidden imaging		
CellNext Solutions	www.cellnext.com	Cellnext Solutions Ltd., +91 11 2681 8445; connect@cellnext.com			DMS
Complete Inspection Systems	www.completeinspection.com		Hidden imaging	Optical taggant	

DNA Technologies	dnatechnologies.com			Chemical taggant	
DNA Tecnologies Pty Ltd.	www.dnatecaus.com			Chemical taggant; Optical taggant	
Dunmore Corp.	www.dunmore.com		Security seals		
DuPont Authentication	www2.dupont.com/Authentication/en_US/	E.I. DuPont India Pvt. Ltd.; +91 12 4254 0900	Holograms & security seals		
FractureCode Corporation	www.fracturecode.com				DMS
Guangzhou Mingbo Anti-Forgery Technology Co. Ltd.	www.mingbo.com.cn/english/gsx.htm		Overt imaging		
HoMAI (Hologram Manufacturers of India)	www.homai.org	HoMAI Secretariat; +91 98 182 81116; info@homai.org	Holograms		
Honeycomb Relationship Management	www.gainsindia.com	Honeycomb Relationship Management; +91 22 2497 6405; vsrinivas@hcrmservices.com			DMS
Honeywell	www.honeywell.com	Honeywell International India Pvt. Ltd., New Delhi	Hidden imaging		
Inksure Technologies	www.inksure.com	Indian Agent: EIPR India Ltd.; +91 22 6630 8495; zk@antipiracy-india.com		Optical taggants	
JDSU	www.jdsu.com		Overt imaging		
JURA JSP GMBH	www.jura.at/en/index.htm			Optical taggant	
Kavach	www.kavach-your-brand.com	PRS Permacel Pvt. Ltd.; +91 22 6635 8333; contact@kavach-your-brand.com	Security seals; overt & hidden imaging	Optical taggant	
Kezzler AS	www.kezzler.com	Indian Agent: PAC Med Biotech Pvt. Ltd.; +91 98 316 72789; avi@pacmed.ca			DME
KURZ Transfer Products	www.kurzin.com	KURZ (India) Pvt. Ltd.; +91 11 2517 0909; sales@kurzin.com	Holograms; security seals; overt imaging		
Label Systems Authentication	www.lsauthentication.com		Holograms; overt imaging		DMS
Molecular Isotope Technologies	www.naturesfingerprint.com			Chemical taggant	

Nanolnk	www.nanoguardian.net			Nanotaggant	
Nanoventions	www.nanoventions.com	Indian Agent: Brady Company India Pvt. Ltd., +91 80 6658 2900; anitha_p@bradycorp.com	Overt imaging		
Nolax	www.nolax.com		Security seals		
OAT Systems	www.oatsystems.com/	OATSystems Software India Pvt. Ltd.; +91 80 6659 5200		RFID	
On+Qor Secure	www.onqor.com		Security labels		DMS
OpSec	www.opsecsecurity.com		Holograms; overt imaging		DMS
OVD Kinegram AG	www.kinegram.com		Overt imaging		
Owens Illinois	www.o-i.com		Specialized packaging		
Payne Security	www.payne-security.com	Payne (India) Pvt. Ltd.; +91 80 2846 7641; bangalore@payne-worldwide.com	Holograms & security seals; overt & hidden imaging		
RFIDAI (RFID Association of India)	www.rfidai.org	RFIDAI; +91 11 6567 7001; info@rfidai.org		RFID	
Schreiner ProSecure	www.schreiner-prosecure.com		Holograms & security seals		DMS
SICPA SA	www.sicpa.com	SICPA India. Ltd.; +91 11 2335 5243	Overt & hidden imaging		
Signe S.A.	www.signe.es		Overt & hidden imaging		
Spectra Systems Corp.	www.spsy.com			Chemical taggant; optical taggant	
Tesa Scribos	www.tesa-scribos.de/eng	Tesa Tapes (India) Pvt. Ltd.; +91 22 2756 4139	Holograms & security seals		DMS
TÜV Rheinland	www.brm.tuv.com				DMS
U-Nica	www.u-nica.com/		Overt & hidden imaging	Nanotaggant	DMS
UPM Raflatac	www.upmraflatac.com	Indian Agent: UPM-Kymmene India Pvt. Ltd., +91 22 2686 7100	Security seals	RFID	
Verify Brand	www.verifybrand.com				DMS
Vesdo Security Technologies	www.vesdo.com				DMS
Visible Assets Inc.	www.visible-assets.com			RFID	
Water Ink Technologies Inc.	www.waterinktech.com		Overt imaging	Optical taggant	

Notes

about us

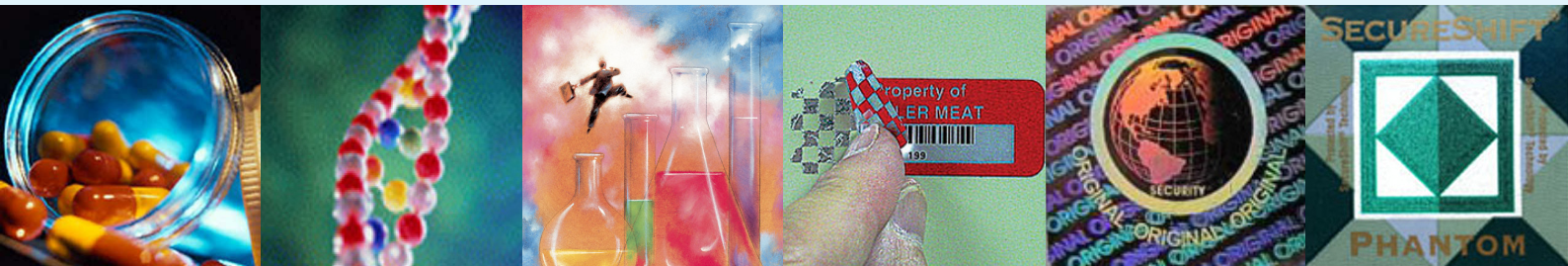
The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the growth of industry in India, partnering industry and government alike through advisory and consultative processes.

CII is a non-government, not-for-profit, industry led and industry managed organisation, playing a proactive role in India's development process. Founded over 113 years ago, it is India's premier business association, with a direct membership of over 7500 organisations from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 83,000 companies from around 380 national and regional sectoral associations.

CII catalyses change by working closely with government on policy issues, enhancing efficiency, competitiveness and expanding business opportunities for industry through a range of specialised services and global linkages. It also provides a platform for sectoral consensus building and networking. Major emphasis is laid on projecting a positive image of business, assisting industry to identify and execute corporate citizenship programmes. Partnerships with over 120 NGOs across the country carry forward our initiatives in integrated and inclusive development, which include health, education, livelihood, diversity management, skill development and water, to name a few.

Complementing this vision, CII's theme "India@75: The Emerging Agenda", reflects its aspirational role to facilitate the acceleration in India's transformation into an economically vital, technologically innovative, socially and ethically vibrant global leader by year 2022.

With 64 offices in India, 8 overseas in Australia, Austria, China, France, Japan, Singapore, UK, USA and institutional partnerships with 271 counterpart organisations in 100 countries, CII serves as a reference point for Indian industry and the international business community.



Confederation of Indian Industry

249-F, Sector -18, Phase-IV, Udyog Vihar, Gurgaon – 122015, INDIA

Tel: +91-124-4101044 / 4014060-67 • Fax : +91-124-4014057

Email: ciico@ciionline.org • Website: www.cii.in

Reach us via our Membership Helpline: 00-91-11-435 46244 / 00-91-99104 46244

CII Helpline Toll free No: 1800-103-1244