

Challenging Your Assumptions Concerning Authentication

Adopting a Bulletproof Solution to Beat the Counterfeiters - and the Lawyers

**By R. James Assaf, Esq.
General Manager
InkSure Inc.**

Brand owners' opinions often differ concerning the features that they value most in an anti-counterfeiting system. Some brand owners prefer unique overt features; others prefer covert features that do not change packaging design and remain hidden from counterfeiters. For some, speed of authentication is a primary driver. For others, authentication through forensic analysis is of paramount importance. Fast to adopt, seamless to apply, easy to train, simple to use: these are qualities that would seem to be incompatible with the brand owner's demand for a solution that offers the highest possible accuracy and security.

Of course, all brand owners agree on one thing: it has to be affordable. Fortunately, one authentication technology has emerged that offers all of these benefits, and more. Covert, machine-readable technology ("CMRT") from InkSure Technologies provides the bulletproof solution that not only defeats the counterfeiters, but the growing reaches of the personal injury attorneys as well.

Change Your Approach

For many brand owners, the current state of brand protection technology being employed is hardly "state of the art." Inertia has taken over, so that standards seem to be determined by what has been done in the past, rather than what is possible now. As a result, brand owners are wasting money on technologies that offer little to no security value, while believing that they are actually saving money by not investing in supposedly higher priced alternatives. However, in this modern age of counterfeiting, with incidents of counterfeiting sharply on the rise and the skill of counterfeiters also increasing dramatically¹, traditional approaches can no longer be considered as commercially-reasonable attempts to prevent counterfeiting. Simply keeping up with the Jones's is not enough to

defeat the new breed of counterfeiter, not to mention the even more vicious personal injury attorney, whose client - grievously suffering the effects of counterfeit medication - inspires great sympathy from a jury looking for the proverbial "deep pocket." Now is the time to demand more from your authentication solutions. No longer is "just good enough" good enough.

The risk managers and company counsel within major corporations can see the battle coming. The brand owner's greatest exposure to counterfeiting liabilities will not occur in the factory, the distribution centre or the street, but in the courtroom. The first salvo has already occurred. In April, 2001, two HIV patients who had unknowingly taken counterfeit Serostim (a human growth hormone used to counteract some of the wasting effects of AIDS) sued Serono

(Serostim's manufacturer) as well as their local pharmacy and Cardinal Health, the Serostim wholesaler. Among their claims, the plaintiffs alleged that the defendants should have foreseen the potential entry of counterfeits into the drug distribution chain and taken preventative measures. The suit was ultimately settled², so one can only conjecture as to the court's ultimate disposition.

More recently, in April 2006 another significant case involving counterfeit drugs and the issues of manufacturer, wholesaler and pharmacy liability was also settled out-of-court. Timothy Fagan filed suit against Amgen, AmerisourceBergen and CVS in August 2003 to recover damages for injuries and suffering caused by his ingestion of counterfeit Epogen following an emergency liver transplant. While the negligence claims against Amgen were dismissed by the

¹FDA counterfeit drug investigations increased from five per year in the late 1990's to over 20 per year since 2000. Combating Counterfeit Drugs: A Report of the Food and Drug Administration, February 2004.

²Katherine Eban, "Pharmacy Fakes: Your Prescription Drugs May Not Be What the Labels Say They Are," San Diego CityBeat, at <http://www.sdcitybeat.com/article.php?id=830>.

³Fagan vs. AmerisourceBergen Corp., et. al., 356 F.Supp.2d 198 (E.D.N.Y. 2004)

Federal district court applying New York law, the claims against AmerisourceBergen and CVS were allowed to continue³. Nick Beckett from the law firm of CMS Cameron McKenna argues that all participants in the pharma supply chain, including manufacturers, should exercise caution in light of the Fagan case: "Nonetheless, it appears that such a claim [against a pharma manufacturer] could succeed in other circumstances and other jurisdictions.... [A cause of action of negligence] may be brought against any member of the supply chain who has breached a duty to take reasonable care. Negligence is not concerned with the product itself or its quality. It will not be a defense for members of the supply chain to argue the goods supplied were not theirs and that they therefore should not be held responsible for them. Rather, members of the supply chain will be under a duty to conduct themselves to a reasonable standard of care to prevent harm to persons whom it might reasonably be foreseen will be affected by their actions. Precisely what constitutes 'reasonable care', to whom the duty extends, and what constitutes a 'foreseeable risk' are questions to be resolved. In the meantime, all those in the supply chain should exercise caution and ensure all reasonable steps are taken - and are seen to be taken [emphasis added] - to minimise the risk to patients."⁴

Publicised incidents of pharmaceutical counterfeiting continue to occur, with alarming frequency. Two major incidents of Procrit counterfeiting were investigated by the FDA in 2002 - 2003, a probe into a major Lupitor counterfeiting ring was launched by Pfizer and the FDA in May of 2003, and three separate Serostim counterfeiting incidents occurred between late 2000 and May, 2003. In November, 2005, 51 packages of counterfeit Tamiflu - used as a precaution to treat Avian flu - were seized by U.S. officials⁵. On October 13, 2006, the FDA issued a nationwide alert concerning the national distribution of counterfeit One Touch brand blood glucose test strips⁶. In many of these cases, the counterfeit packages were virtually indistinguishable from the original, including

the use of holographic safety seals, lot numbers and stamps. Common themes of these incidents include vulnerable points in the mainstream drug chain that allow counterfeiters to insert their products undetected; lack of vigilance by manufacturers, wholesalers and dispensers; the extreme sophistication of counterfeiting techniques; the difficulty of distinguishing counterfeit from original; the lack of a centralised alert system that quickly, efficiently and widely informs parties of the counterfeit danger; and finally, the serious health risks that these counterfeiters pose to innocent victims⁷.

Brand owners are now on notice that the risk to their supply chain is real, that "traditional" solutions are not successful in eliminating these risks, and that the consequences of inadequately securing the integrity of their product's distribution are foreseeable and can be disastrous to individual consumers. The elements for a prima facie case of negligence are readily available to the eager plaintiff's attorney. The fact that the brand owner may not know of any specific counterfeiting schemes, and has taken token steps to secure its packaging, may not be enough anymore to avoid liability. "Even if each link in the distribution chain denies knowledge or participation in the counterfeiting scheme, perhaps it can be argued that their sheer negligence in assuring the pedigree and safety of their drug batches places them at fault, as well."⁸

Where can a brand owner find guidance on how best to assure the safety of their products? Certainly, the FDA would be considered an authority in this area. Utilising an approach that adopts the recommendations of the FDA would be a positive step toward meeting the standard care by which authentication programs will be judged. Throughout the final report of the FDA's Counterfeit Drug Task Force entitled *Combating Counterfeit Drugs* (October 2004), the FDA emphasises the need for multi-layered authentication solutions, with particular positive emphasis on the use of taggants as well as on forensic technologies.

The FDA's conclusions regarding authentication technologies are as follows:

"Due to the high costs and technical barriers that authentication technologies create for counterfeiters, their use is a critical component of any effective multi-layered anti-counterfeiting strategy, especially for products that are likely to be counterfeited.... Existing authentication technologies have been sufficiently perfected that they can now serve as a critical component of any strategy to protect products against counterfeiting.

- The use by manufacturers and repackagers of one or more authentication technologies on their products, particularly those likely to be counterfeited, would protect the public health and diminish counterfeiting;
- To facilitate the use of authentication technologies on existing products, FDA plans to publish a draft guidance on notification procedures for making changes to products (e.g. addition of taggants [emphasis added]), their packaging, or their labeling for the purpose of deterring and detecting counterfeit drugs;
- FDA plans to continue to evaluate and disseminate information to stakeholders on developing forensic technologies (e.g., use of product fingerprinting, addition of markers) [emphasis added] and other analytical methods that allow for rapid authentication of drug products."⁹

The FDA has laid out the various elements that it believes form the basis for an effective anti-counterfeiting system: multi-layered, addition of taggants, use of forensic technologies, and rapid authentication. These features should be incorporated into a bulletproof authentication technology that allows for forensic-level accuracy (i.e., meets the requirements for court admissibility), yet is easy to use and provides for definitive field authentication in seconds. Moreover, the technology must be virtually impossible to counterfeit - even the most high-tech simulations must be unable to fool it. In addition, the technology must not be dependant upon the collective security of all of its users - no technology user should be able to compromise the security of a different

³Nick Beckett, "Technology, Media & Telecoms: A Bitter Pill," *Legal Week.com*, June 16, 2005

⁴Brand Journal, vol. 5, issue 4 (May/June 2006), p. 6

⁵U.S. Food & Drug Administration press release no. P06-167, October 13, 2006

⁶Jennifer Ann Lee, "Counterfeit Drugs: A Growing Public Health Risk in Need of a Multi-factored Solution," page 26.

⁷Id., page 20.

⁸Combating Counterfeit Drugs, supra note 1.

Special Feature

user of the technology.

I believe that only InkSure's CMRT solutions provide all of these features, allowing for field-forensic authentication of custom security "codes" that are unique to the brand owner. InkSure's solutions guarantee NO FALSE ACCEPTS, ensuring confidence in the authentication program by security personnel. InkSure CMRT technology enables fast and definitive field audits, allowing the brand owner to conclusively prove that it is utilizing best practices to ensure that its distribution chain has not been breached by counterfeits. InkSure's SignaSure™ and PocketSure™ readers can be distributed to field personnel or third-party professional auditors (available through InkSure) with no threat of compromise to the security of the solution. InkSure's CMRT solutions provide Level II (covert machine-readable) and Level III (forensic) authentication within the same product; in addition, InkSure's SmartInk can be combined with Level I (overt) devices such as holograms and colour-changing inks to provide all three levels of authentication protection within a single device. For the brand owner who is serious about protecting his customers and his company from the risks of personal injury and loss of revenue caused by counterfeiting, maybe it is time to abandon "tried and not-true" traditional approaches to authentication, and to embrace a comprehensive multi-layer solution which includes InkSure CMRT.

Consider Your Alternatives

Why are traditional authentication solutions inadequate? The use of overt technologies alone provides two shortcomings: ease of simulating the overt effect, and difficulty of training the audience for which the features are intended. Because overt technologies are, by definition, visible, the counterfeiter does not need to waste any energy in identifying the anti-counterfeiting feature. Therefore, half of his job is already done. Technology now allows almost any visual effect to be replicated, if not exactly, then closely enough to fool most viewers. It is common knowledge that most holograms have lost much of their security value due to the ability of counterfeiters, particularly in the Far East, to

counterfeit the devices. Hologram manufacturers will counter by saying that the latest holograms incorporate a variety of features that make true counterfeiting impossible. However, these arguments point out the true fallacy of a dependence on overt features alone.

The leading overt techniques employ the use of optically variable devices, or OVD's. These include holograms and colour-changing inks, features that provide some optical variation or change based on an external stimulus, such as a changing viewing orientation or the application of heat or cold. The "authenticator" - generally the consumer, personnel in the distribution chain or security personnel - has to determine the authenticity of the overt device based either on general

“... reliance on overt devices alone will not discharge the duty of care owed to the public to ensure product integrity.”

familiarity with the product and prior use and experience with the OVD, or by comparing it to a template or a list of instructions supplied by the brand owner. Both of these approaches are problematic. In fact, the assumption that consumers can distinguish a real OVD from a fake is truly the "emperor's clothes" of the authentication world. While an astute consumer may be able to recognise a very poor counterfeit, the consumer - and even most security personnel - cannot readily distinguish the real OVD from the good counterfeit with the unaided eye. How could they, without detailed instructions? There simply is no good way to educate consumers on how to distinguish good OVD's from bad (although some try with web site directions, the efficacy of which cannot be established). In fact, some of the overt effects in OVDs are so subtle that even trained personnel in the authentication industry have difficulty accurately identifying them (is that a true colour "flop" or simply a shadow from changing the viewing angle?). Some programs try to compensate by providing authenticator personnel with comparison templates or detailed instructions. However,



Signasure

not only does this create more complicated training and slower field authentication, but the use of templates and

instructions serves as "how-to manuals" for counterfeiters. A security program is only as strong as its weakest link, and all it takes is for one list of instructions to be lost or purposely forwarded to a counterfeiter for the entire program to be compromised. While overt solutions do have their uses - particularly as a first layer in a more complex authentication program - reliance on overt devices alone will not discharge the duty of care owed to the public to ensure product integrity.

Perhaps recognising the shortcomings of overt features, brand owners, for some years now, have begun turning to covert authentication features, either as standalone security devices or in conjunction with overt devices. However, over time these devices have fallen into two camps: mass-produced devices that have lost their security value, or forensic solutions that are not easy to use (and therefore have little practical value).



Pocketsure

Perhaps the most common covert feature is UV ink. This ink - actually a dye or taggant that is mixed into other inks or varnishes - is invisible under normal conditions, but can be illuminated with black lights. UV ink has become a victim of its own success: because it is so common, is easy to identify with readily available lights and is equally easy to procure, it has lost almost entirely its security value, and is now more effective as a means of internal process control, rather than security. UV inks have been replaced by IR (infrared) "upconverters" as the commodity covert device of choice. However, common IR taggants are following the same historical curve as UV ink before it. Since there are very few versions of these taggants, they are widely distributed to numerous customers, from numerous suppliers. They are widely available to anyone, including counterfeiters. They are easy to recognise through the use of commonly available laser pens. (One additional drawback of this technology - many

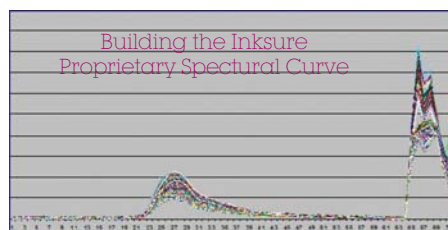
Special Feature

IR laser pens pose a health risk, since their beams are invisible to the naked eye, but can cause serious retina damage.) While some brand owners combine overt features with commodity IR taggants or UV inks, they are simply increasing their costs without receiving any real return for such investment. "Not secure" plus "not secure" does not equal secure. "Not secure" plus "not secure" will not protect consumers, and will not insulate the brand owner from liability.

"Forensic" markers, on the other hand, such as organic and synthetic DNA, binding pairs, micro-taggants and other similar technologies, do not suffer generally from the mass distribution that has ruined the security value of UV dyes and IR upconverters. However, these technologies offer either slow or no field authentication. Some of the DNA authentication technologies offer multi-step field authentication procedures, in which encoded labels are first activated with specialised markers, and then read with field authenticators. This is a destructive test: the encoded label is permanently discoloured once authenticated. Micro-taggants require the use of microscopes to detect the taggants, and the judgment of security personnel to determine whether the micro taggants exhibit the appropriate characteristics. The slow speed of such authentication methods prohibits the use of these technologies in high-throughput applications such as pharmacy and return centre audits. While these markers can be definitively identified in a laboratory, brand owners do not need to invest in extra markers for this purpose: they are generally capable of identifying their own products via laboratory forensic testing without the need of additional markers. What brand owners need are field readers that offer forensic-level protection, which only InkSure can provide.

Besides InkSure, a few other companies offer CMRT taggant solutions that are not based on the use of commodity UV or IR upconverters. However, none of these companies offer the degree of accuracy or security of InkSure's CMRT solutions. These competing CMRT solutions all suffer from incidents of false accepts, where the authentication reader incorrectly identifies a label, package, product or random object as

an authentic item. Because of the relative simplicity of the optics in these technologies (generally CCD or single photo diode receptors), other objects can "mimic" the signals that the reader is expecting to see. InkSure's SignaSure reader, on the other hand, utilises a combination of a mini-spectrometer and multiple filtered photo diodes to provide up to 75 data points in distinguishing the authentic "covert fingerprint" from the unmarked product, the attempted counterfeit, and the random object. InkSure guarantees "no false accepts." This is critical in ensuring the success of the authentication program. If security personnel find that their reader is incorrectly identifying unmarked items as authentic, they will quickly lose confidence in the system and will stop using it. Perhaps more importantly, if a reader



signals a false accept on an unmarked object, how will it respond to a true counterfeit attempt?

In addition, other CMRT providers are limited in the number of taggants/formulations that they offer their customers. As with UV dyes and IR upconverters, the security of their solutions suffers with their success. As more of their customers use the same few taggants, each customer becomes more dependent on the security practices of the other customers with whom they're sharing the authentication code. As use of the few taggants becomes more widespread, the possibility of a counterfeiter learning of its employment also becomes greater. Rather than trying to reverse engineer the taggant, the counterfeiter will simply target one of the many locations where the taggant is being used, in order to procure its own supply. One CMRT provider markets the security of its solution by advertising the low concentration percentage of its taggant. However, given the limited number of taggants that it has available, the provider is actually providing a cookbook to

counterfeiters who, if able to procure the taggant from one of its many sites, will now know exactly how much taggant to use in its counterfeits.

InkSure, on the other hand, provides unique, custom SmartInk™ formulations to each of its customers. Unlike other CMRT technologies that build their technology around a small collection of "unique" markers, and remain limited by those markers, InkSure has developed its technology around the industry's most flexible reader. InkSure readers operate on multiple frequencies, and each reader is configurable, so that those frequencies can change depending upon the specific formulation designed for the customer. As a result, InkSure can work with a multitude of materials, both organic and inorganic, and can leverage the latest in chemistry science, such as the use of nano particles. InkSure can develop the specific formulation that best meets the requirements of customer's specific application, including environmental and printing requirements. Because each customer can receive its own specific formulation, it is not dependent on the security of other InkSure customers. If an InkSure customer suffers a breach of its own security, only its program is impacted (and InkSure can respond quickly by providing a new custom formulation and reader reprogramming, if necessary). InkSure offers the unique combination of a commercially proven technology that is nonetheless exclusive to the brand owner.

Confound Your Adversaries

First and foremost, an anti-counterfeiting system must beat the counterfeiters. This means the solution must beat them in the streets - no reverse engineering - and beat them in the courtroom - it must provide iron-clad court-admissible evidence. It should be covert, or contain covert elements, to make the counterfeiter's job more difficult. It should allow for secure supply chains, to protect against theft of the security taggants. It should be mobile and fast, to allow for large-scale field audits as well as the immediate authentication of suspect items. And it must be forensic, to ensure the highest degree of accuracy and to meet the requirements for the

Special Feature

admission of scientific evidence.

InkSure custom SmartInk formulations are virtually impossible to reverse engineer. The SmartInk is covert: InkSure taggants cannot be seen with the naked eye, nor can they be illuminated with UV black lights or IR laser pens. Even if the counterfeiter ultimately learns where the SmartInk is located, he will not be able to identify and/or recreate the actual taggants used. Even highly expensive forensic tests will not successfully aid the counterfeiter. Spectrophotometer analysis may identify certain fluorescent emissions from the encoded product, but will not reveal the specific fluorescent profile of the covert fingerprint for which the reader is programmed, nor the taggant composition and taggant/ink/substrate combination required to replicate such fingerprint. With spectrophotometry, some taggant emissions could look like common objects, while conversely other emissions from the ink or substrate could look like part of a unique code (but are not). Other forensic tests, such as ICP-AES, ICP-MS and SEM-EDAX, can succeed in identifying unique elements even in parts-per-trillion concentrations, but such tests are easily contaminated, do not distinguish taggant elements from ink and substrate elements, and do not identify actual molecules. Since there can be many permutations of elements within taggant molecules - different ratios of elements per molecule, etc. - trying to recreate a taggant from this information alone is like trying to recreate Mozart's Symphony No. 40 from just the raw musical notes, without possessing the sheet music or having heard the actual composition.

In addition, InkSure's use of custom formulations for each of its customers greatly diminishes any benefit that a customer could achieve, even if reverse engineering were possible. With competitive technologies, a successful replication by the counterfeiter would allow him to infiltrate the supply chain of all of that technology's users, perhaps justifying his investment in the reverse engineering process. However, with InkSure's custom CMRT technology, the counterfeiter would realize that even the most complex and expensive reverse engineering program would impact only a single InkSure customer.

The cost of trying to defeat the InkSure solution would far outweigh any benefits in succeeding. The counterfeiter would quickly determine that it is more profitable to focus on defeating the non-custom authentication products.

Because of the security of the InkSure solution, the brand owner has the option of utilising the technology as a deterrent - "advertising" the fact that the technology is being employed, so that counterfeiters do not even attempt to copy the product - or as a means of actually catching the counterfeiters. InkSure's CMRT technology provides the elements that will enable a brand owner to prosecute the counterfeiter to the fullest extent of the law. These three elements - secure distribution of the security technology, demonstrably reliable authentication methodology, and maintenance of standards and measurements to ensure program compliance - form the "Forensic Triangle," the foundation of a bulletproof forensic system.

A true forensic system should utilise markers that are secure from the hands of counterfeiters. InkSure's custom SmartInk formulations are virtually impossible to reverse engineer, and their limited distribution means that the taggant supply chain remains secure. Counterfeiters will take the path of least resistance: rather than investing in costly, time-consuming reverse engineering efforts with no guarantee of success, they will instead try to identify a commodity taggant by using a black light or IR laser pen, and then purchase that taggant on the open market. In addition, even for taggants that are not illuminated with common devices, the counterfeiters may simply use their market intelligence resources to target the supply chain of known suppliers of a limited number of formulations. InkSure's supply chain is solid: its readers will only positively authenticate the brand owner's specific custom code, and it will only ship the brand owner's exclusive chemistry formulations to the brand owner's specified printers/converters.

In addition, InkSure's CMRT technology meets the requirements to the admissibility of scientific evidence expounded by the U.S. Supreme Court. In *Daubert v. Merrell Dow Pharmaceuticals*¹⁰, the Supreme Court set forth a four-pronged reliability test that a court

should consider in determining whether evidence should be admitted:

1. Can - and has - the evidence been tested?
2. Has the theory or technique been subjected to peer review and publication?
3. Is there a known or potential rate of error, including the existence and maintenance of standards for the technique?
4. Is the technique generally accepted in the scientific community?

InkSure's CMRT utilises the analytical technique of spectrophotometry, which measures the unique frequencies that selectively excite certain substances, and the different frequencies that are then emitted by such "excited" substances. Spectrophotometry meets the Daubert requirements for reliability: it has been utilised in forensic labs for years; is employed by various forensic instruments including emission spectrographs, mass spectrometers, visible spectrometers, infrared spectrometers and x-ray diffraction spectrometers; is widely accepted in the scientific community; has been the subject of numerous publications and peer reviews; and is a technique that allows for the quantitative testing of evidence of maintenance of standards in its application.

InkSure's spectrophotometric methods can utilize up to 75 data points in its field-forensic *SignaSure* readers to measure emissions from selected illumination wavelengths. It utilizes proven, accepted techniques for distinguishing marked from unmarked products. Any items that fail to match the covert fingerprint profile at any one of the 75 data points will cause a "reject" indication. The technology's robust code development and quality control systems provide quantifiable data to establish accuracy and error rates.

Other CMRT technologies may have difficulty in meeting the Daubert tests for reliability. While some "novel" technologies may sound sexy, are they based on techniques that have been generally accepted in the scientific community? Does the technology provide for the existence and maintenance of standards by which it can be measured? Have the techniques been subject to peer review and publication? In addition to the court's tests for reliability, will

¹⁰509 U.S. 579 (1993)

Special Feature

the technologies meet the brand owner's requirements for no false accepts?

In a court action against a counterfeiter, the brand owner (or the prosecutor, in a criminal case) must prove two things: (1) that the counterfeit item does not contain the CMRT code, and (2) that all legitimate products do contain the CMRT code. Therefore the bulletproof authentication solution must not only provide a forensically-detectable authentication code, but also a system for proving that the counterfeit products absolutely would have been encoded with the CMRT fingerprint, had they been authentic. In addition to providing a secure supply for security markers and demonstrably reliable scientific methodology, InkSure's CMRT meets the third leg of the forensic triangle by offering ruggedized quality assurance systems. These systems not only provide real-time assurance to the authorised printer that SmartInk application is being performed per specification, but also automatically generate data that definitively documents the proper application of the CMRT code to all items in a product line or batch. InkSure's 6-Sigma level quality control solutions have been developed in cooperation with manufacturing experts including DuPont Authentication. InkSure's Q.A. solutions include its high-speed SortSure readers, which can be mounted in fixed positions or on a traversing arm over printing webs to provide real-time hands-free 100% verification or sampling of the SmartInk application, with automatic alarm generation if the code emissions fall above or below established limits. Off-line SignaSure QA handheld readers are also available. In either case, quality control data is logged by date, time, taggant emission levels and, in the case of SortSure, web location, for quality assurance reference as well as for court evidence of the proper calibration of authentication equipment and application of the SmartInk to all intended items.

Confirm Your Authenticity

Most authentication technologies would have the brand owner believe that there are two elements to a successful anti-counterfeiting solution - the overt or covert authentication device, and the method for confirming the presence of the authentic device (e.g., visual inspection, CMRT reader).

However, having the means to authenticate the product, without actually using such tools in a systematic matter, does nothing to ensure the integrity of the distribution chain. In fact, mere application of an authentication device alone, without some manner of systematic field inspection, may actually increase the risk of liability, since it encourages those handling the product throughout the distribution chain, from wholesalers and distributors to pharmacists and even consumers, to rely too heavily on the use of such device without making any separate effort, no matter how minimal, to confirm the product's legitimacy.

The bulletproof authentication program must show that authentication is, in fact, occurring - in locations and at a frequency designed to provide a commercially reasonable sampling of the product's distribution. In addition, this "sampling" should be documented, to provide evidence of the brand owner's proactive efforts to ensure that counterfeiters have not infiltrated its distribution chain. Field audits can occur by waiting for the distribution chain to funnel products to inspectors - such as in return centres - or by taking inspectors to the products, such as distribution centre or pharmacy audits.

InkSure's authentication readers are the perfect tools for use by security personnel or third-party auditors for field inspections. SignaSure readers can read up to ten exclusive SmartInk codes, and utilize forensic analysis to definitively authenticate products in less than two seconds. SignaSure provides "red light / green light" visual indicators, audible tones and LCD readouts to identify the product being authenticated. PocketSure readers are customized to read a single SmartInk code, are small enough to carry in a pocket, and are priced competitively with much less sophisticated or secure IR laser pens. Because inspectors do not have to identify or interpret the authentication feature themselves - they simply place the InkSure reader on the product, press "Execute" and immediately receive the definitive indication of authenticity from the reader - they can accurately sample large populations of product much more quickly than with any other authentication method. In addition, authentication data can be downloaded from SignaSure for use as evidence of program compliance and reader performance for program quality assurance and

litigation purposes.

SignaSure readers provide flexibility, so that brand owners can utilize them in a variety of ways, from large-scale field audits to covert internal inspections that are secret even to normal security personnel. However, for the brand owner that does not have sufficient resources for its own field audit program, InkSure can provide third-party auditing services that can utilize InkSure readers to quickly inspect products in pharmacies, distribution centres and other locations.

Commence Your Activities - NOW!

The bulletproof authentication solution is available to the brand owner now. InkSure solutions have been in commercial use for five years and provide all the products and support necessary for immediate implementation. Brand owners are at risk of a major liability incident at any time. Don't take a bullet when the bulletproof solution can provide your customers and your company with immediate protection.

Covert, multi-layered, fast, forensic, mobile, and definitive: CMRT solutions from InkSure Technologies provide the features that the brand owner needs to defeat the counterfeiters - and the attorneys.

About the Author

R. James Assaf is the General Manager for InkSure Inc., the sales and marketing subsidiary of InkSure Technologies Inc. Mr. Assaf has a background in commercial law, having run the commercial law practice of Sensormatic Electronics Corporation, the world leader in loss prevention technologies, for eight years. Prior to Sensormatic, Mr. Assaf worked as an associate attorney for the international law firm Squire, Sanders & Dempsey. Mr. Assaf graduated second in his class at Case Western Reserve University School of Law. His law review Note, Mr. Smith Comes Home: The Constitutional Presumption of Openness in Local Legislative Meetings, 40 Case W. Res. L. Rev. 227 (1989), is a referenced resource at Vanderbilt University's First Amendment Center and is listed in the syllabus of the "Political Regulation" course at the University of California, Berkeley.

Reader Enquiry 19