As originally published in the SMTA International Conference Proceedings.

STRATEGIES FOR FIGHTING COUNTERFEIT ELECTRONICS PRODUCTS

James R. Williams, Ph.D.
Polyonics, Inc.
Westmoreland, NH, USA
jim.williams@polyonics.com

ABSTRACT
The author provides a framework for analysis of the necessary choices brand-owners must make, to protect their brands from product counterfeiting activities. A new paradigm for fighting counterfeit electronics is presented, based on the existing strengths brand owners have in today's supply chain.

Key words: Brand Protection, anti-counterfeiting, track and trace, product authentication, covert technology, taggants

SCOPE OF THE PROBLEM – OVERVIEW
"Counterfeiting is the dark side of the electronics industry, and the gloom is spreading…The problem affects virtually all companies along the supply chain, from component suppliers to distributors, EMS providers, ODMs, OEMs, and their customers", stated *the San Jose Mercury News* in 2004. Numerous books, articles, market research reports, and studies have been written to document the facts: counterfeit goods now account for 6-8 % of global production (in excess of $ 300 billion in 2008), and accounted for 750,000 lost jobs, according to a US Commerce Department study. Moreover, this means that fake products cost electronics manufacturers approximately $ 20 billion dollars in 2008. More importantly, fake electronics are finding their way not only into consumer electronic products, but also into medical instrumentation and national aerospace and defense systems![1]

SOME BASICS
Numerous brand protection case histories based on successes and failures from other industries have established certain fundamental truths.
First, there is no "single solution (often referred to as "the silver bullet") which, by itself will successfully deter counterfeiting of products. Restated, "there is no single technology which by itself, cannot be defeated". More importantly, these same case histories have lead to the widely accepted principle of "layered technologies", by combining overt, covert, and forensic technologies as the foundation for successful brand protection;
Second, product counterfeiting has become a global "business," impacting every manufacturing sector and product type imaginable, and is growing exponentially. This is a "business" of deception and appearances, i.e. to sufficiently convince a prospective buyer by the **appearance** of the fake product, that it is the "genuine" product, to pay for it. Ideally, the counterfeiter will remain undetected "long enough", and not be caught.
Third, each brand owner typically offers broad product lines, and must make tradeoffs regarding which counterfeited products present the greatest risk to their firm, which type of technology should be used to protect/deter, to what extent counterfeiters should be prosecuted (vs. deterred, for example), and how to allocate resources accordingly.
Fourth, these choices must be made in an environment rich in conflicts. Conflicting constituencies exist within each brand owner's corporate structure, i.e. who "owns" it, and is responsible for solving the problem? Oftentimes the brand owner can not, or will not, choose to acknowledge that they even have a problem due to these conflicts;.
Fifth, current recognition of counterfeiting as a "global war" has been compromised by prior years' widely used euphemistic characterizations such as "knock-offs", or "replicas" to describe fake consumer luxury products. Consumers seem to tolerate poor product performance as long as the consequences of product failure are inexpensive or trivial. However, when human health and personal safety are involved, our tolerance for fraudulent products is "zero". Many argue that there should be "zero tolerance" for all fakes, no matter how inconsequential poor performance is. Counterfeiters, like all human beings, are greedy. Experiencing success with one type of fraudulent product feeds the counterfeiters' ambitions to move on to other, more lucrative products, even including those which present significant health and safety risks to the buyers.
Finally, all available information unequivocally reveals that WE ALL have a counterfeit product problem, exacerbated by the global outsourcing environment throughout the electronics manufacturing supply chain. Therefore, "we all must assume responsibility for the integrity of the supply chain." The time to rally to the common cause and take collaborative action is today, rather than find a comfortable "blame" to attach to someone else.

IT'S ALL ABOUT TRADEOFFS
Fighting counterfeiters is similar to the situation encountered when two hikers are confronted simultaneously by a grizzly bear. The first goal is not to outrun the bear, but to outrun the other hiker. Eventually, perhaps, you must worry about the bear. Deterrence of attack on my company's well-defended products will undoubtedly result in a shift of these attacks to other, less protected brandowners. Indeed, we must continue to pursue legal remedies and criminalization of counterfeiting activities, through governmental actions to "increase the costs of doing business" for the counterfeiter. In the meantime, each

company's first strategic goal must be to minimize the current and potential risk of harm to your brand, in the most cost effective way possible.

STRATEGIC ELEMENTS

The purpose of a strategy is to move from our current situation to a "more desirable future state, with well defined goals", in an orderly, yet flexible and adaptive fashion. Successful implementation depends on clear understandings of "where we are today", where we want to be tomorrow, the actions needed to get us there, and how to measure our success along the way, in order to adjust our strategy according to periodic successes and failures. To accomplish this, we need to maximize our strengths, minimize our weaknesses, and focus our resources on those priorities which we MUST DO, to achieve our goals. Tactically we also must know the strengths and weaknesses of our competition or opponent, to take advantage of their weakness while avoiding their strengths, i.e. we must "out-strategize the counterfeiter's strategy".

THE COUNTERFEITER'S STRATEGY

A counterfeiter, like any other business person, wants maximum ROI with the least amount of risk. However, the counterfeiter's strategy is to convince the buyer to pay for a product which appears to be legitimate, when it is not. This strategy is "perception driven". A label which is legitimate does not guarantee the contents of the corresponding packaging, only that "it looks real". This is particularly true in electronics manufacturing, i.e. oftentimes fake components and materials are packaged in re-cycled, but original, authentic packaging or containers. Complex situations and multiple markings increase the chances of someone observing an imperfection in the appearance, thereby increasing the odds of the fake product being detected, ***before it is paid for.*** The counterfeiter relies on repetitive information on products or packages, which can be duplicated cleanly and rapidly with a battery of readily available digital technologies, which can give faithful reproduction of the original information and images, so that the products will appear to be legitimate. The counterfeiter will take advantage of 'confusion' within our supply chain, due to widespread geographic locations, and multi-tiered subcontracting and outsourcing between companies. These normal business activities mean actual physical loss of control of data or physical product at these interfaces, once they leave your direct 'span of control', i.e. your manufacturing facility, operated with your own (presumably trustworthy) staff. Every physical movement of sub-assemblies and products between two firms creates opportunities for entry of fake products and loss of information, within your supply chain.

Counterfeiters thrive on "business as usual" attitudes. For example, revenue recovery is most often stated as the first goal of most brand protection programs. This usually results in lengthy and detailed, classic "ROI" justifications, in a classic "B-School" style. From the counterfeiter's perspective, this means that if "I can steal from you less than that amount which will meet your hurdle rate for ROI, I will continue to steal from you". Moreover, counterfeiters rely on the corporate inertia, due to anxiety over potential liability claims against 'your company' if you incorrectly accuse someone of counterfeiting activities.

Many companies argue that "our competitor may gain an economic advantage, if it is known that "we have a counterfeiting problem" ….while the competitors assert that they do not. *The data overwhelmingly shows that we all have a problem, whether or not we choose to recognize it, or address it.* Notwithstanding the available data from multiple sources, a recent study by the Brand Protection Council, revealed that half of the brand owners surveyed acknowledged that they had a problem and were willing to make the long term investment required to eliminate it.

IT'S ALL ABOUT INFORMATION

Since the strategy of a counterfeiter is "all about appearance of authenticity", the counterfeiter's resources and "R&D" are dedicated to ***simulating the appearance*** of legitimate products. As a result, another fundamental truth has emerged from successes in the pharmaceutical industry: "Mark or identify everything you possibly can [on the product] with authentication features, including bottle caps and tops, information inserts, labels, containers, packets, pouches, packaging, as well as markings on the product itself, 'even at the capsule or tablet' dose level". This provides multiple opportunities for "more sets of eyes" to increase the probabilities of spotting a fake product.

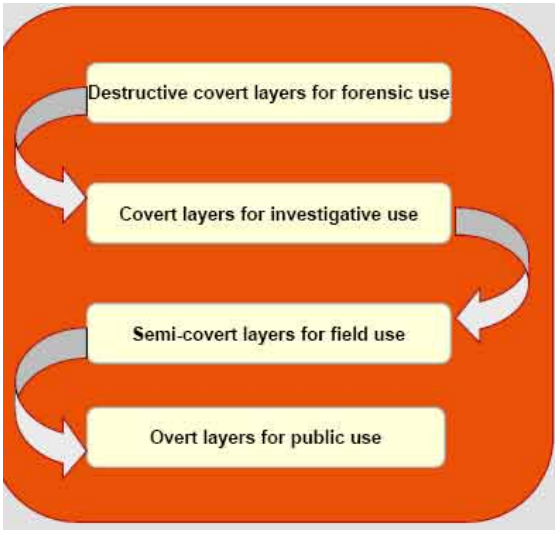
DEFENSES OF THE PAST TO FIGHT THE WAR OF THE FUTURE?

There is a saying in military circles, to the effect that" generals plan the next war based on their results of their last one." History is replete with examples which show the folly of such planning, for example the Revolutionary War in the US (open field volley fire vs. guerilla warfare), and the Maginot Line in France (easily finessed by combinations of the use of tank warfare and airpower). Many brand protection forums today address the issues of "avoiding or detecting" counterfeit products and components, so that bad parts will not be used in our manufacturing operations. Historically, SPC methodologies have served us well as a shield against bad quality incoming parts and components, as well as for products we sell to others, i.e., six sigma, lean manufacturing, and the like. I'll suggest that relying solely on this is equivalent to fighting the war against counterfeit electronics based on our successes from the past wars (improving product quality). In my opinion, this is insufficient for the "new wars" of Brand Protection we are now involved in. Rather, it is a defensive strategy, reminiscent of "fighting from a fixed position", based on our successes. It is susceptible to "flanking maneuvers", as the French experienced with the Maginot Line of France in the run-up to World War II. To my way of thinking, this parallels the counterfeiters' successes to date.

The counterfeiters have a wide array of new technologies available in order to compromise or “flank” our defenses. Examples include digital photography, digital printing, the internet, as well as a plethora of laboratory capabilities to “reverse engineer” and circumvent existing standard product protection technologies, coupled with widespread “computer hacking” for unauthorized access to confidential information, information alteration, and the like. Certificates of compliance can be forged, data can be altered, and unauthorized products “look identical” to authorized ones.

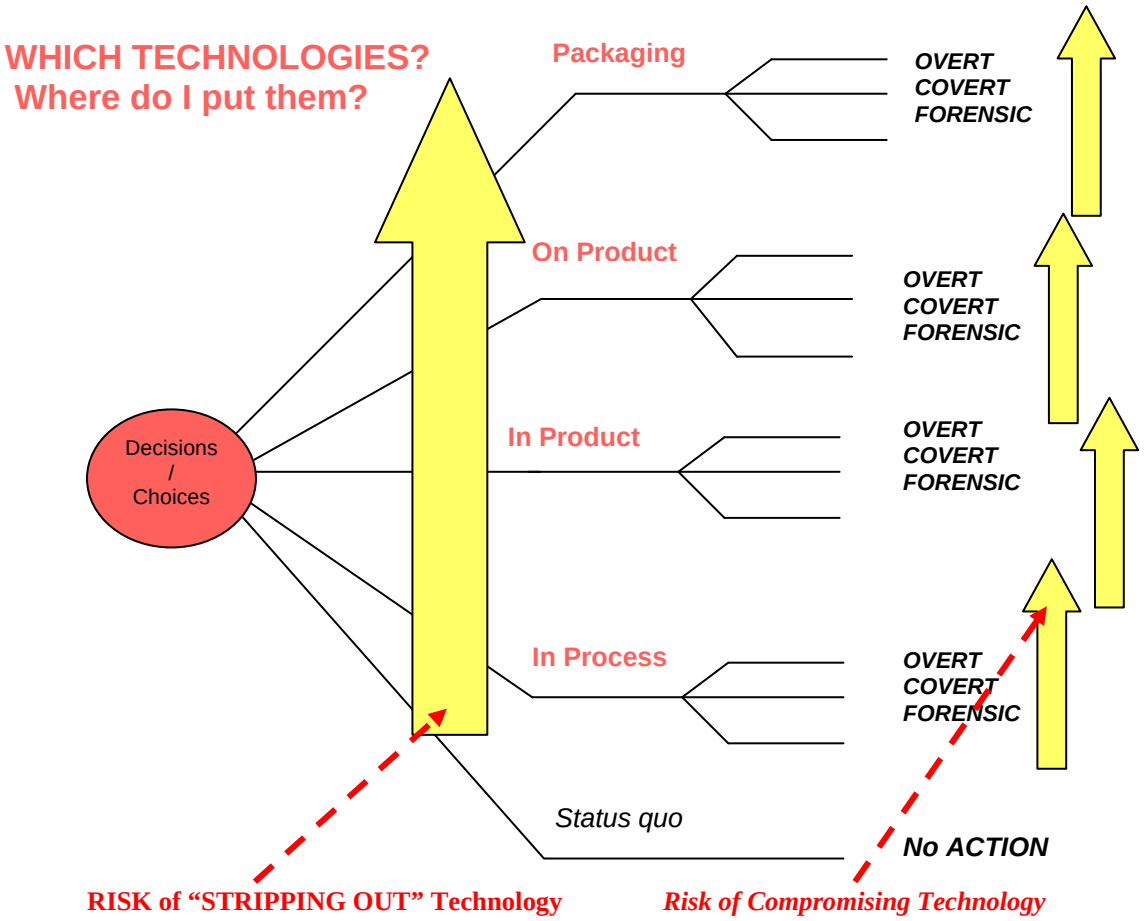
The primary weapons available to fight counterfeiting are technologies which provide information about the authenticity of a product. Dozens of effective technologies are now available. ***Overt technologies*** are those which are readily visible to the naked eye, including ordinary consumers. ***Covert technologies*** are those visible only when viewed or scanned with a proprietary, portable instrument of some kind, typically used in field investigations. ***Forensic technologies*** are used when irrefutable information is needed which will withstand scrutiny in a legal proceeding. Each technology has strengths and weaknesses associated with it, again requiring that tradeoffs must be made by the brandowner before brand protection programs are undertaken.

Successful brand protection programs rely on using different layers of technology, for different purposes, as depicted below:



Technology choices should be made only after the brandowner decides what to do with the information gathered. For example, deterring consumers from purchasing products because they “look different” is a completely different strategy from ”I’ll catch the counterfeiters and send them to jail”. The fundamental questions the brandowner must answer are:1) what is the value of the information you are looking for; and, 2) what will you do with the information once you have collected it?

Moreover, where and how the product is marked also entails choices and tradeoffs. Figure 1 organizes these issues into the form of a “Decision Tree” to help understand and organize the tradeoffs involved.



Overt technologies are the most visible and readily seen by customers, thereby giving instantaneous authentication results. Examples include holograms. This means that the brandowner has a "field investigation team" (consumers) at virtually no cost, but they must be trained, somehow. However, because of their high visibility, overt technologies are more readily copied (or compromised). ***Forensic technologies*** are inherently the most secure, because of their sophistication and difficulty to detect. "If the counterfeiters don't know what it is, and how to detect it, then they can't compromise it." The tradeoff here is the cost and time involved in getting authentication results, since normally the product under suspicion must be sent to a laboratory for analysis, using auditable "chain of custody" methodologies. ***Covert technologies*** are particularly useful in providing a balance between speed of result, and risk of compromise. However, covert technologies usually require portable equipment, to be used only by authorized personnel, which increases operating costs, and limits the size of the field investigation effort.

LOCATION OF FEATURES

Likewise, the ***choice of location*** for the brand protection technology on the product influences its security level. If security labels are placed on *external packaging*, it can be removed. In the case of recycled packaging, counterfeit products can be repackaged in legitimate, but re-used brand protection packaging. Technologies physically *on the product* are somewhat more secure, because the counterfeiter runs the risk of marring authentic product, in attempts to remove the markings (for example labels). Moreover, as in the case of remarking electronic components, the counterfeiter now must invest significant efforts to match product markings on products***, to the same high marking standards required by the original manufacturer.*** Component suppliers and users have developed high levels of sophistication in examining components and other parts for tell-tale signs of remarking. Incorporation of security features literally *in th e product* are even more secure, because now the counterfeiter must truly invest not only in efforts to understand the technology used for protection, but also how to integrate the "compromising technology" into the fake product. Now, the work required (along with investment and risk) goes beyond the scope of the original strategy. Finally, incorporating brand protection technologies as an integral part of the manufacturing process provides the most secure "positioning" location, because the counterfeiter must not only simulate the appearance of the authentic product, he must figure out how to incorporate it into the product itself. So, it's "time to move on" to easier targets.

STRATEGIC IMPLICATIONS FOR ELECTRONICS MANUFACTURERS

Electronics manufacturers are already using elements of “new weapons systems”, which I believe can be adapted to use in “the next war”. Automatic bar code data collection is widely used throughout the electronics manufacturing world, clearly in shipping and receiving, between customer and vendor. It is also widely used globally for individual company’s process and materials control, in real time, as an integral part of automated manufacturing processes. This widespread and extensive use pre-adapts electronics manufacturers for “track and trace” technologies, beginning at the WIP level, for all companies using bar code data collection.

With correctly configured bar code data collection, one can expect: 1)Real time product information, at each step of the manufacturing cycle; 2)Batch codes, date codes, plant location, which shift, even which operator; 3)Since the “on-line” printing processes, such as thermal transfer printing, ink jet printing, are digital processes, ***encrypted/unique numbers*** can be assigned to individual parts, subassemblies, as an enhancement to existing product identification practices; 4) Products are already labeled or otherwise identified, and the data is scanned by others, either internally within your own company, or externally by your sub-contractors or customers; and, 5)Technical information as well as business information is commonly exchanged between sub-contracting partners, with established transaction protocol handshakes.

PREADAPTATION FOR TRACK AND TRACE AT THE WIP LEVEL

Dr. Steven Simske at HP has used the idea of "pre-adaptation" in dinosaurs[2] as a conceptual framework for anti-counterfeiting discussions. Basically, all birds came from one species, that, although earthbound, was a "feathered" animal. The feathers originally were for warmth. Yet, all birds came from this species because the feathers pre-adapted each subsequent generation for flight.

Barcode labeling is widely used in many manufacturing operations, in a real-time environment, for manufacturing processes. According to CACP labels are the 'media' of choice to carry authentication/security features for up to 75 % of products manufactured. Obviously barcode labels are a ubiquitous element in many manufacturing operations. In fact, most electronics manufacturers view the barcode label with its data as a component of the respective subassembly, assembly, and product.

What's involved in barcode identification of products, in real-time? Product information is printed on a label, and it is applied to the corresponding product or subassembly in a specific 1-to-1 relationship. Downstream, the barcode data is scanned and the information is used as an integral part of manufacturing operations.

An authentication feature (for example a so-called 'taggant') can be readily included as part of the label material or as part of the ink. The new operating paradigm is modified to be "Product [and authentication] information is printed on a label, and it is applied to the corresponding product in a specific 1-to-1 relationship. Downstream, the product [and authentication] data is scanned and the information is used for the intended purposes of the manufacturer [brandowner]."

PREADAPTATION AT WORK !!

A few changes will necessarily be required. The brandowner must add an additional field (Authentication) in the database. In addition, a new scanner must be used which will not only scan the existing barcode product data, but also detect (or scan) the authentication data. Since the aforementioned brand owners now will use the pre-existing AutoID technologies to include the authentication component, a major shutdown/re-tool for implementation is avoided. Everything being labeled now, can also be authenticated and/or tracked, by taking advantage of this "pre-adaptation".

This concept also addresses "common factors for successful brand protection strategies." Label or identify 'everything you can" with authentication features...and "Plan for evolution of features over time." Using “taggants”as a conceptual model, the program starts by incorporating a taggant in the ink or ink ribbon. Later on, the same (or a different) taggant can be incorporated into the label material. Finally, two independent taggants can be used, one in the ink and one on the label. Moreover, technology is also available which relies on detection of two independent taggants, in a specific ratio, simultaneously, in order to get authentication. What better place for proportional structures than in a barcode image?

Because the elements of track and trace for the barcoded products are in place throughout the distribution channels and supply chains (existing barcode data collection systems and EDI technologies) massive changes in existing operations are minimized. And, the brandowner now has the opportunity to have product data and authentication data from the birth of the product throughout the distribution channel, and to the final user. These elements pre-adapt, or pre-position us, to authenticate products from the moment of their birth, within an operating network of authorized participants, dedicated to authentication of products at every stage. Some changes will be required, of course. The authentication information can be incorporated into the ink, the label material, or both, in an orderly progression. Operationally, no other changes are necessary. The normal scanners used must be changed to not only include scanning of the product information, but also scanning of the authentication information. Likewise, databases must be changed to include a field for authentication, which is then permanently linked with the corresponding product information, which is that being collected today.

These changes can be done stepwise, even on a "pilot basis". For example, if you want to determine whether or not you have a product diversion problem, products can be labeled with authentication-enhanced labels, for example, to be shipped only to one location. If that product appears in unauthorized channels, by the appearance of covert scannable labels appearing "where they are not supposed to be", you now have concrete evidence of a problem. This type of field test would only require changing to an enhanced ink ribbon or label stock, and equipping your field investigator with the proper, portable scanner for the investigative work.

UNIQUE SERIAL NUMBERS WITH HANDSHAKE PROTOCOLS

Technologies are in place which would enable the equivalent of an "e-pedigree" for every component, sub-assembly, and product. Unique numerical identifiers are now being accepted as one weapon to be used, even at the consumer level, to validate the authenticity of a product, prior to paying for it. One brand protection model advocates a scenario in which a consumer would take a picture of a 2D barcode identifier on a product, and upload the photograph to the appropriate secure network server. Upon validation, the consumer would proceed to checkout, with the confidence of buying the authenticated product.

Following the example of many "continuous product quality improvement" programs, we can view the movement of a product during its manufacture from one work center to another, as a series of handshake transactions between "internal customers". Authentication can occur at every step, including movement of the sub-assemblies to outside manufacturers, and the return of product back into assembly operations. The intrinsic value of all these transactions is that authentication information can be explicitly and uniquely linked with specific product information, for every unit manufactured, throughout the manufacturing process, and to the retail level.

CONCLUSIONS

The problem of counterfeit electronics is global, with enormous economic repercussions for the electronics industry. It affects us all. Denial does not work. Pointing to independent distributors is not identifying the root cause, but reacting to a symptom. The industry is pre-positioned to move away from its defensive posture without major disruptions to operations. Technologies utilized within our existing infrastructure indicate that strategies can be formulated which can mitigate the effects of counterfeiting.

ACKNOWLEDGEMENTS

The author wishes to thank the following individuals for their contributions, critique and input: Dr. Steven Simske, Hewlett Packard Corporation; Mr. David Howard, Johnson and Johnson; Mr. Neil Sellars, National Label Company; and, Mr. David Brown, Intel Corporation.

REFERENCES

[1] *"Dangerous Fakes"*, Business Week, http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm
[2] http://en.wikipedia.org/wiki/Preadaptation