

“Fendi sues Walmart for sales and distribution of counterfeit goods.” If we’re not careful, this could be a very common headline. In this series of articles we’ll examine the use of Information Technology practices in fighting counterfeit.

Background:

Most sources agree that counterfeit products are stealing approximately 500 billion dollars of annual, legitimate revenue. This directly equates to loss of legitimate jobs, loss of tax revenue, loss of brand quality and even the loss of life.

Loss of Life? Counterfeit materials used in planes, construction and brakes for example, can directly lead to loss of human life. Counterfeit parts in a plane do not live up to FAA inspection requirements. Defective brakes will not stop a vehicle efficiently and perhaps not at all.

Counterfeit drugs prevent patients from receiving proper dosages of medicine. Most counterfeit drugs involve “cutting in” some other chemical or element with real medicine resulting in a 10-20% of actual dose. Who knows how harmful the rest is?

In China 9 out of 10 DVD/CDs sold are counterfeit. While this is not life threatening, it is a major issue and one that needs to be resolved.

The Reactionary, Stop Gap Measures:

The immediate reaction to counterfeit is to embark on a grandiose strategy to mark and track every good made by a company. Most companies today do not mark their products with anything permanent. Perhaps the closest thing to date would be a barcode that has many other uses as well.

There are many different permanent and temporary tags available: elemental tags (organic and in-organic), molecular tags, random particle patterns. Tags can also be engineered to be responsive to different energies such as X-Ray Fluorescence (XRF) or Infra Red Light (IR) or Ultra Violet Light (UV) or even water or a known solution. Each has advantages and disadvantages.

Presently, there are patents held by many organizations in each of these categories. Some have been issued in the US and some in China. As China continues its move to the world stage, expect more and more patent issues as Chinese filings predate US awarded patents. This will be an interesting issue for China and the rest of the world. Patents awarded when China was a far more closed society could be used to pre-date and then invalidate US issued patents. If China was closed, should those US businesses forfeit their patents based upon the filing?

All of these marking technologies have a place in the anti-counterfeit market. Even combining tag technologies to create a more complex tag could and should be used to help protect a product.

Advancement of the art in this area will yield independent, item level tags that are random in

nature and not created or engineered by humans. This will allow for more information to be carried on the item such as the difference between a barcode and a two dimensional data matrix often referred to as a 2D barcode.

The problem is that each of these stand-alone strategies is hackable and spoofable. There are labs all across the world with the technology to identify the elements in a tag. Reproducing certain molecules would appear to be harder, but still, they can be copied. In some cases, such as XRF based tags, the estimates of time required to copy them are in the hours, not even days.

“One upmanship” is a must. Anti-counterfeit product providers must stay one step ahead of all counterfeit efforts. This will yield a very high turnover and obsolescence strategy. For example, is a simple IR scanner is designed to read a certain tag, once that tag is no longer in use or the IR strategy employed by that company changes, the scanner is now obsolete and must be replaced.

A marked product and an independent, stand-alone scanner is merely a front line of defense. A more complete strategy must be employed to truly be effective protecting a brand and limiting if not eliminating counterfeit items.

Where Does Information Technology Come In?

Like computer viruses, counterfeit products have a way of working their way into supply chains when we don't even know they there. All computers in a company should be protected with Anti-Virus technology. So should the supply chain be protected from counterfeit items.

Most large organizations utilize some type of Enterprise Resource Planning (ERP) system such as SAP or Oracle. The inventory systems in these applications can serve as a second line of defence.

Companies with shipping and delivery infrastructures should be able to spot item quantity anomalies fairly easily. Suppose a warehouse receives 1000 cases of item A and ships 2000 cases of item A. Unless there were 1000 cases of item A in the starting level we have a problem. Scenarios like this should be checked regularly and are fairly easy to spot as common sense and logic can be powerful weapons. Simple reports or pattern searching algorithms will make this job easier.

The more difficult scenario is when employees steal from their company. Suppose that warehouse receives 1000 cases of an item. Then those real items are removed and replaced with 1000 cases of counterfeit goods. Aside from visual monitoring of the warehouse, what system can spot that? RFID, nope. Tagged products with scanners, nope. Perhaps if we integrate the front line scanners with a back end database...

Scanners interfaced with backend computer systems have the advantage of looking at a product logically over time and in it's location. Today, manufacturers tag products with unique serial and lot numbers to allow tracking them as best they can. Each item will have a unique

Written by Administrator

Friday, 13 March 2009 18:00 - Last Updated Friday, 13 March 2009 18:34

identifier that will allow the manufacturer to pull up history of that product assuming that the information exists in a database somewhere.

Vehicle Identification Numbers (VINs) are great examples. Each and every time a vehicle is in an accident or even worked on, a transaction related to the vehicle is and can be generated and stored in searchable databases. So, before purchasing a used car, for example, one can obtain the VIN number and perform a search to retrieve an accurate history of that vehicle. Why not apply the same thing to products?

A company can internally or with the help of an independent firm, build a database to track its products. Suppose a certain lot was created in China and imported to the US via Oakland. Or, that was the supposed track. If a group of those products came in through the Port of Wilmington in Delaware, what should happen? We now have an anomaly that's easily identifiable using a scanner that's tied to a back end system. The items coming in through Delaware are clearly counterfeit, as the company and item's information states via shipping manifests and such that the items from that lot were to come in via Oakland. At the very minimum a flag should be raised.

In each case the counterfeiters will look to "spoof" the tracking systems by inserting products with false identification. With proper IT capabilities and the application of real world logic, this process can be made quite difficult. For example, if a product serial number was scanned coming off of a production line in China on Monday, it should not be scanned in Oakland on Tuesday, unless there is a special circumstance. Spotting these abnormal conditions in the supply chain is relatively easy with a strong IT infrastructure. These exceptions can then lead to notifications or merely tracked in a database to begin building trend data.

That trend data is the real solution to counterfeiting. Determining whether or not a product is real is important, yet will do little to prevent counterfeiting. Determining where the holes existing in business supply chains is the real key. Just like legitimate businesses, counterfeiters need distribution and sales channels to be successful. Careful monitoring of the supply chain will enable businesses to prevent counterfeit products from entering the chain, thus eliminating the counterfeiters delivery and sales channels.

This scenario can be applied anywhere throughout the supply and delivery chain. The more detailed and fastidious a company is in setting up these paths, the more effective they can be against products entering their chain.

Item tags and RFID have their place too.

An item tag can and will work in a similar fashion to an item ID, except that it's readable by a technology other than a bar code or two dimensional data matrix scanner.

Examining tags and RFID we can place them into two generic categories, line of sight and longer distance.

RFID has the distinct advantage over all other tags in that they can be read over the radio

waves and thus, at a distance. When combined with a solid back end system, RFID can prove to be a very strong system. However, RFID can be easily spoofed and destroyed.

When fighting counterfeit items, it's VITAL to capture FAILED reads. This task leaves RFID wondering what to do. If a warehouse supervisor walks around taking inventory with an RFID unit, they will never see a product that does not have an RFID tag. For this reason, visual inspections must occur to ensure the validity of RFID tags.

If not RFID, Then what?

If visual inspections are a requirement, why not use a line of sight product verification device? For one, that could be impractical, but it would be harder to spoof if each product were scanned individually rather than a group scan.

Each item's id would then be queried against the central system to ensure that the product "logic" was sound. For example, if an item ID passes through a checkpoint twice, something happened, or one of the two items is fake. Or for an even more powerful situation, two items scanned in two different cities within an hour. A database of travel profiling could be set up to show that this occurrence is invalid. Two independent scanners side by side could not accomplish this. Integrating them to a backend item flow logic system, however, could and it could do it rather easily.

This requires technology that walks the line between database access device and scanner. A scanner that's designed to collect information and post it to that central, long term database for that trend analysis should be a medium term goal for all organizations to begin blanketing and policing their supply chain.

The Employee Gotcha

One of the keys to success for such a system is a double-blind approach. This allows scanning, verification and collection of data without disclosing too much information to operators.

Data collected can only be trusted in the hands of trusted people. Chain of evidence rules in the US highlight this problem. Additionally, if employees have too much information about what's being inspected when and how, it positions them to help spoof the system by ensuring all of the counterfeit goods are removed from the facility to be inspected.

The best solution to this problem, is to audit products covertly. The two dimensional data matrix scanner, for example, appears and runs just like a normal scanner. The fact that it also has the ability to verify particle pattern product verification needs not be disclosed to the employee base.

Similar to police detective techniques, it may be more valuable to track the counterfeit item to learn more about the people involved. Development of a back end database application can help organizations drive home this ability. Covert data collection will prevent the employee base

Written by Administrator

Friday, 13 March 2009 18:00 - Last Updated Friday, 13 March 2009 18:34

from even knowing whether or not a product is specifically collected. In fact, it's really no concern to them, as it's not part of their daily job.

So what's the Solution?

This is the trickiest question of all. There are many companies that claim they have the solution, yet none really do. There is no magic wand to solve this problem. Counterfeit is a global problem and is here to stay. There is simply, no simple solution.

Consumer awareness and brand inventory management are key. So much data is already being collected by sales and inventory systems. Proper analysis of that data will provide major clues to holes in the supply chain.

Of course, technology continues to evolve and develop. While there is not clear leader in this space, and most companies are at the vaporware and promise stage, technology development continues in this area. The big boys will likely enter this market when viable technologies have been developed. They'll follow the standard model such as innovate internally or acquiring small companies who have worthwhile technology, although there are few, if any currently.

It's worth following.

Mr. Koffenberger is currently an independent consultant. He spent much of 2005 and 2006 working on anti-counterfeit systems worldwide. He can be reached here:
jt.koffenberger@delmarvagroup.com