An Auto-ID Based Approach to Reduce Counterfeiting in the U.S. Pharmaceutical Supply Chain

by

Indy Chakrabarti

B.S. Electrical Engineering
Rice University 1997

SUBMITTED TO THE ENGINEERING SYSTEMS DIVISION FOR PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN LOGISTICS

AT THE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MAY 2003

© 2003 Indy Chakrabarti. All rights reserved.

The author hereby grants MIT permission to reproduce and distribute publicly paper and of this thesis document in whole or in part.

Signature of Author: ____________________________________________
Engineering Systems Division
May 9, 2003

Certified by: ____________________________________________________
James Masters
Professor of Logistics, MIT
The thesis supervisor

Accepted by: _____________________________________________________
Yossi Sheffi
Professor of Civil & Environmental Engineering
Co-Director, Center for Transportation and Logistics

Compiled March 2003

LIBRARIES
An Auto-ID Based Approach to Reduce Counterfeiting
In the U.S. Pharmaceutical Supply Chain

By

Indy Chakrabarti

Submitted to the Engineering Systems Division
on May 9, 2002 in Partial Fulfillment of the
Requirements for the Degree of Master
of Engineering in Logistics

Abstract

This thesis will discuss a new approach to preventing the adulteration of prescription medicines in America. The primary thrust of the solution is based on research conducted at MIT’s Auto-ID Center on radio frequency technology. The United States faces a growing threat to patient health due to the increasing rate of counterfeit medicine being introduced into the legal pharmaceutical supply chain. This has long been an unresolved global problem, but only recently has it become a major threat in America. Existing legal and technical efforts to control counterfeiting are no longer sufficient to contain the problem. The threat of counterfeits can be partially ameliorated by installing RF-capable electronic tags onto medical packaging, and creating a unique electronic product code (EPC). RF tags though, are not the only component of the required solution. New legal actions, better use of existing technical countermeasures, and industry cooperation are also required. This thesis will outline in more detail the interplay of each of these components in developing a robust solution to the problem of counterfeit medicines.

Thesis Advisor: Jim Masters
# Table of Contents

## I. The Problem of Counterfeit
- Introduction ................................................................................. 6
- Comparison of Counterfeit Operation to Authentic Operation .......... 6
- Problem Definition ....................................................................... 7
  - The WHO Definition of Counterfeit ........................................ 7
- Size and Scope of Problem .......................................................... 8
  - Global Scope ........................................................................... 9
  - Asia, Asian Sub-continent and the Pacific Rim ......................... 10
  - Europe ..................................................................................... 11
  - South America ........................................................................ 12
  - Africa ....................................................................................... 12
  - United States ......................................................................... 13
- Legal Initiatives ........................................................................... 13
  - Prescription Drug Marketing Act ........................................... 14
  - Prescription Drug Price Parity for Americans Act (H.R. 4614/S. 2244) 16
  - Drug Importation Act of 2002 (H. R.5186) .............................. 16
- Notable Examples of Counterfeits ................................................ 17
- What Gets Counterfeited ............................................................... 19
  - Classes of drugs reported as counterfeit from 2000 through 2001 (WHO) 19
  - Types of tampering reported from 2000 through 2001 (WHO) .......... 19
  - Recent Counterfeit Incidences Compiled by the International Chamber of Commerce 20
  - Counterfeit Products Reported In US During 2001 – 2003 from FDA MedWatch 20
  - Incidences of Counterfeiting Reported by the HDMA .................. 21
- Industry Response ...................................................................... 21
- A Solution to the Problem ............................................................ 22
- Methodology .............................................................................. 23

## II. Existing Non-RFID Based Anti-Counterfeit Technologies
- Introduction .............................................................................. 24
- Types of Anti-Counterfeit Technologies ....................................... 25
  - Overt Technologies .................................................................. 26
  - Covert Technologies .................................................................. 27
- Intra-Formulation Techniques ...................................................... 28
  - Immunoassay ........................................................................... 28
  - Flavor ...................................................................................... 29
- Package Level Techniques ............................................................. 30
  - Design ..................................................................................... 30
  - Watermarks ............................................................................. 31
  - Fibers and Threads .................................................................... 32
  - Reactive Inks .......................................................................... 32
  - Holographic (OVD) ................................................................... 33
  - Numeric - Bar Code .................................................................. 34

## III. Overview of RFID Technology
- Introduction .............................................................................. 35
- Rough Cost Estimate for One Possible RF-ID Implementation ........ 38
- Cost Estimate for First Year RF Implementation for Manufacturer .......... 38
- Summary of Costs by Recurring and Startup by Percentage .......... 40

Compiled March 2003
IV. Preventing, Detecting, and Resolving Counterfeits

Overview of Solution

Legal Changes
Industry Regulation
Punitive Measures

Greater Vigilance
Supply Chain Members
The FDA
Police Force
Medical Community

Supply Chain Cooperation

Non RF-ID Based Technical Countermeasures

V. Using RF-ID as a Countermeasure

RF-ID as Counterfeit Prevention
Automated Authentication
Difficulty of Replication

Overview of Proposed Solution Architecture
Diagram of RF-enabled Supply Chain
Manufacturer Database
Audit Database
Local Database

Manufacturer Components
Ingredients Suppliers
Bulk Pharmaceutical Manufacturers
Dosage Pharmaceutical Manufacturers
Example of a Basic Manufacturer EPC Descriptor File in MDb
Open Information: Track & Trace
Open Information: Product Description
Example of Basic Audit Database EPC Record
Secured Information: Highly Restricted Access – FDA
Manufacturer Level Privilege: Upstream Tracking
Manufacturer Level Privilege: Downstream Tracking
Distributor Level Privilege: Upstream Tracking
Distributor Level Privilege: Downstream Tracking
Retailer Level Privilege: Upstream Tracking
Retailer Level Privilege: Downstream Tracking
Returns Handler Privilege: Upstream Tracking
Returns Handler Privilege: Downstream Tracking
Transportation Provider T1
Medicine Authenticator A1
Example of Basic Local Database (LDb) Record for a Manufacturer
Distributor Component
- Pass-Through Distributor
- Break-Bulk Distributor

Retailer Component

End User Component

Other Supply Chain Members
- 3rd Party Return Handlers
- 3rd Party Authentication Firms
- 3rd Party Transportation Providers
- Non-RF-Capable Intermediaries
- Governmental Organizations

Counterfeit Detection within a Fully RF-Enabled Supply Chain

Counterfeit Detection within a Fully RF-Enabled Supply Chain
- Table of Scenarios
- Scenario 1: Introduction of fake EPC by Distributor Diluting Product
- Scenario 2: Counterfeit Product Shipped by Internet Pharmacy
- Scenario 3: Using Returned Products For Counterfeit
- Scenario 4: Dumpster Diving – Retrieving Empty Containers for Counterfeit
- Scenario 5: Selling Expired Product as Authentic
- Scenario 6: Selling Sample Product as Authentic
- Scenario 7: Diversion – Selling Products from an Authorized Channel to an Unauthorized Channel
- Examples of Counterfeit Detection using Alternative Technologies and AutoID
- Scenario 8: Package Tampering
- Scenario 9: Formulation Tampering

Supply Chain Coordination with Members Without RF Infrastructure

VI. Conclusion

References
I. The Problem of Counterfeit

Introduction

A growing problem worldwide and the United States is the introduction of counterfeit medicines into the legal supply chain\(^1\). This thesis will define the problem, provide examples of counterfeiting, discuss existing actions taken and technologies available to reduce the incidences, outline a new strategy to combat the threat, and provide a rough estimation of the associated costs.

*Comparison of Counterfeit Operation to Authentic Operation*

Counterfeit Operations for Making Fake Panadol

---

\(^{1}\) "Counterfeit Drugs Pose An Increasing Danger", *Chain Drug Review*, 19\(^{th}\) Nov. 2002.

Compiled March 2003
Problem Definition

There are many conflicting views on what constitutes a counterfeit product. Some industry experts include spoilage of a product due to improper storage as a form of counterfeiting. For the purposes of this thesis, the World Health Organization’s definition will be used.

*The WHO Definition of Counterfeit*

“A medicine that is deliberately and fraudulently mislabeled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may..."
include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient active ingredients or with fake packaging.²"

According to the WHO definition, what makes a drug/medicine counterfeit is the deliberate or intentional (criminal) nature of the mislabeling or adulteration of a product. For the purposes of this thesis, improper storage and maintenance producing a substandard drug will not be judged to be counterfeit. The later problem is a parallel issue that can also be mitigated by the implementation of an RF infrastructure but not discussed here. Diversion involving labeling changes, for example, by taking a drug meant for the French market and changing its labels to English and selling it in the U.S., will be treated as counterfeiting. On the other hand, diverting product without making any alterations to the product will not be viewed as counterfeit. The resale of expired products is included in the definition of counterfeit.

This thesis will focus only on securing the domestic pharmaceutical supply chain. A global solution is needed, but the infeasibility of getting concurrence at the global level requires that a domestic solution be implemented in advance of reaching this consensus. This proposal will discuss countermeasures to the threat of counterfeits based on implementing a combination of legal changes, business practice changes, and implementation of both RF and non-RF based technical solutions. It will also advocate a graduated approach to implementation of the proposed solution in consideration of the financial and technical constraints of the industry players involved.

Size and Scope of Problem

---

² World Health Organization Feb 15, 2003  
http://www.who.int/medicines/organization/qsm/activities/qualityassurance/counterfeit/faq_counterfeit.doc  
Compiled March 2003
The World Health Organization estimated several years ago that between five and eight percent of the worldwide trade in pharmaceuticals is counterfeit\(^3\). However, most experts believe this to be a conservative estimate and that the total amount of counterfeit is increasing. The health impact of this problem is already significant. Reconnaissance International, publisher of Authentication News, states that criminal pharmaceutical counterfeits have killed thousands of persons worldwide. The motivation for this criminal activity is simply the huge profit potential that exists in selling counterfeits that of high priced medicines. The relatively lax control over the drug supply chain makes it easy for counterfeit operations to survive unmolested, and the high price that prescription pharmaceutically can fetch makes it a tempting industry to invade. In fact, anecdotal evidence suggests that some former illegal narcotics dealers are switching to selling fake pharmaceuticals because the margins are just as high, but the risk of getting caught is lower\(^4\)! The HDMA (Healthcare Distribution Management Association), an industry organization, has started taking steps to combat this growing threat. Below is a compilation they have made of examples of counterfeit\(^5\). Their findings, broken out by region, are outlined below.

**Global Scope**

As the incident reports below demonstrate, counterfeit is a global phenomena that has been around for many years. It is already a significant threat in many developing countries

- "Between 1982 and 1997 there were 751 cases reported of counterfeit drugs found in at least 28 countries. In 25% of the cases, the drugs were reported to come from industrialized countries, 65% from developing countries, and 10% from unspecified sources (WHO press release, November 1997)."

• “42 reports of counterfeit products from 20 countries during 2000 and 2001 (WHO, 2002) or 46 reports from 20 countries 60 percent of which came from developing countries (IFPW Focus, June 2002).”

• “According to WHO, between January 1999 and October 2000, they received 46 incident reports from 20 countries, 60% of which were from developing countries (IFPW Focus, 6/13/02).”

• “According to WHO, 5 – 8% of the worldwide trade in pharmaceuticals is counterfeit (Security Management, 9/1/01).”

• “In developing countries, about 25% of drugs are counterfeits (Washington Post, 8/30/02).”

• “GlaxoSmithKline is planning to spend $29 million clamping down on counterfeit versions of their branded products (World Markets Research Centre Daily Analysis, 1/29/03).”

**Asia, Asian Sub-continent and the Pacific Rim**

This region of the world faces some unique challenges from counterfeiting. The incident of fakes is very high and particularly difficult to distinguish. This is because many Asian outfits have the technology required to produce packaging that is very similar to the original product, at the same time, many Asian governments do not have the wherewithal to properly combat this threat.

• “One third of anti-malarial drugs for sale in Cambodia, Laos, Burma, Thailand and Vietnam contained no active ingredient (Lancet quoted by Washington Post, August 2002).”

• “The Government of India has suggested withdrawing state licensing powers and creating a centralized licensing and vigilance system for both manufacturing and trade. The main focus would be to curb the prevalence of counterfeit product (Indian Business Insight, 11/20/02).”

• “A one-year survey in the Philippines found that 8% of the drugs were counterfeit, and 11% of the pharmacies were dealing in counterfeit pharmaceuticals (IFPW Focus, 6/13/02).”

Compiled March 2003
• “China
  
  ○ Approximately 192,000 people died in China in 2001 due to the effects of counterfeit drugs. As much as 40% of drugs in China are counterfeit (Washington Post, 8/30/02).

  ○ In 2001, the State Drug Administration closed 1,300 factories and investigated 480,000 cases involving counterfeit drugs worth $57 million (Washington Post, 8/30/02).

  ○ Despite the activity of the State Drug Administration, there are still approximately 6,500 counterfeit pharmaceutical producers in China (Business China, 1/6/03).”

Europe

European markets are segmented by overall national wealth. Countries with less developed economies, like Russia and Spain, are where a disproportionate number of counterfeits are identified. This presents a threat to the region as a whole though, as lax trade barriers between European nations and the expansion of the EU to less developed nations, increases the likelihood of fake drugs surfacing in any given nation within Europe.

• “The Department of Health and Consumption in Spain has announced that 200 counterfeit pharmaceuticals have been identified on the local market (World Markets Research Centre Daily Analysis, 11/6/02). “

• “Russia
  
  ○ In 1997, there were no reported cases of counterfeit pharmaceuticals in Russia. At current rates of increase, they predict 25% of drugs in the next 2 years will be counterfeit (Agence France-Presse, 5/9/02).

  ○ The AIPM estimates that the total lost revenue in the Russian pharmaceutical market is $250 million out of a $2 billion market (Agence France-Presse, 5/9/02).
o The Russian Ministry of Health has stated that 80 more counterfeit drugs were found on the market in 2002 – up 140% over 2001.

o According to the Main Presidential Control Department, the annual cost of counterfeits in the Russian market is $200 million, or 7% of their market. The Health Ministry states it is less than $220,000 (Prime-TASS, 1/27/03).

o In a report by the Association of International Pharmaceutical Manufacturers and the Coalition for Intellectual Property Rights, it states that 12% of the Russian pharmaceutical market is counterfeit (Agence France-Presse, 5/9/02).

o In 1997, Russian officials only detected one counterfeit, now there are more than 170 (Reuters, 11/29/02).”

**South America**

- “In Columbia, up to 40% of medications are believed to be counterfeit (U.S. News & World Reports, 6/11/01).”

**Africa**

In Africa, the impoverished circumstance of many nations presents a breeding ground for counterfeiters. Governments lack the money and the manpower to scrutinize pharmaceuticals, yet their populations, due to poor health care, suffer from a disproportionate incidence of diseases.

- ‘The Nigerian Representative of Overseas Pharmaceutical Manufacturers donated a fixed wireless hotline phone with Internet and computer facilities to the National Agency for Food and Drug Administration and Control in Lagos. This will facilitate communication about counterfeit incidents and illegal parallel importation (All Africa, 3/8/03). “

- “Approximately 50% of drugs sold in Nigeria are counterfeit (IFPW Focus, 6/13/02).”
United States

As evidence from the U.S. suggests, often the counterfeiting is very localized. The South Florida area has a large cluster of counterfeiters. Florida’s large elderly population, who are large consumers of prescription drugs, present a profitable target for these dealers. Similarly border regions near Canada and Mexico show higher incidences of counterfeits. Therefore, greater vigilance in these geographical clusters is recommended.

- “Of the 1,458 legal wholesalers in Florida, 55 are suspected of selling counterfeit drugs or medicine obtained fraudulently. More than 70% of the wholesalers are located in the South Florida Miami-Dade area (The Miami Herald, 3/5/03). “
- “Governor Bush (FL) has asked the state Supreme Court to empanel a statewide grand jury to investigate the “troubling criminal trend” of drug counterfeiting (St. Petersburg Times, 12/24/02).”
- “Chairman Bliley of the House Commerce Committee states that the FDA only has information on about 18% of foreign drug manufacturers shipping to the U.S. (www.CBSNEWS.com, 12/8/00).”
- In a study conducted at Dulles International Airport and Oakland International Airport, Customs and FDA agents found that 10% of the drugs they analyzed contained no active ingredients (U.S. News & World Reports, 6/11/01).
- 55 counterfeit investigations were opened from October 1998 through June 2002; In the same period OCI opened 255 PDMA diversion cases (FDA Office of Criminal Investigations – July 2002 Hubbard testimony Special Committee on Senate Special Aging).

Legal Initiatives
The FDA and legislators have recognized the problem of domestic counterfeits for a number of years. The following proposed legislations recount some of the attempts taken by the U.S. government. Unfortunately, up till now, the requirement for unit-of-use level tracking that is necessary for counterfeit prevention has been financially prohibitive with current technology. As a result, the pieces of these bills that refer to tracking have been put on hold by the government after justifiable lobbying efforts from the pharmaceutical industry.  

**Prescription Drug Marketing Act**  
In 1988 Congress recognized the dangers of re-importation when it enacted the Prescription Drug Marketing Act (PDMA). PDMA was the result of congressional investigations, led by the House Energy and Commerce Committee. The committee stated, “A significant volume of pharmaceuticals are being re-imported. These goods present a health and safety risk to American consumers because they may have become subpotent or adulterated during foreign handling and shipping.” PDMA’s overall purpose is to “decrease the risk of counterfeit, adulterated, misbranded, subpotent or expired prescription drugs reaching the American public.” Under PDMA, all licensed distributors must have in place detailed storage and handling procedures that address:

- Temperature and humidity control and documentation
- Inspection of incoming and outgoing product shipments
- Rotation of product to prevent expiration
- Employee training in storage and handling of pharmaceuticals
- Extensive background checks on employees
- Facility and product security
- Procedures for handling recalls and returned goods
- Sanitation of facility
- Disaster plans for both inside and outside the facility
- Comprehensive written policies

---

6 Healthcare Distribution Management Association, 14 Apr., 2003  
http://www.healthcaredistribution.org/index.v3page?p=5048  
7 Healthcare Distribution Management Association, 14 Apr., 2003  
Florida, where a great deal of counterfeiting has been detected recently, has spearheaded legislation to reduce the possibility of counterfeit introduction. The Florida legislature has proposed the Florida Pedigree Requirement.

This requirement requires tracking of the following attributes for each lot of medicine:
1. Drug Name
2. Dosage
3. Container size
4. Number of containers
5. Drugs Lot or Control numbers
6. Business Name and Address of ALL parties to each prior transaction, starting w/the manufacturer
7. The date of each previous transaction

Both HDMA and the Pharmaceutical Distributors Association (PDA) made comments concerning the Florida Pedigree Recommendations. While HDMA supported many of the recommendations, it objected to two key elements: “requiring authorized distributors to pass the pedigree on sales of products equal to $200 or more, and the treatment of intra-company transfers.” It cautioned that these requirements could lead to delays, shortages and higher prices. It went on to argue that typical HDMA members carry large numbers (30-40,000) of stock keeping units (SKUs) and that product purchased from secondary sources are typically intermingled with existing inventory. The complexity of maintaining pedigrees on small lots in this situation would be unmanageable and unsupportable with net profit margins of 0.72%. The HDMA also concludes that electronic technologies for this purpose are “just not available today.” Intra-company transfers, it argues, should not be considered sales and therefore should not require a pedigree requirement. This proposal argues that electronic technologies, specifically RF-ID capabilities, can allow industry participants to meet the Pedigree requirements at an acceptable price point if implemented over the next few years.
Additional congressional bills propose that distributors and resellers be allowed to re-import drugs from abroad. This conflicts with legislation that attempts to minimize the incidence of counterfeit, as re-importation is a key driver in the introduction of counterfeits into the supply chain.

*Prescription Drug Price Parity for Americans Act (H.R. 4614/S. 2244)*

The “Prescription Drug Price Parity for Americans Act” (H.R. 4614/S. 2244) would allow pharmacists and pharmaceutical wholesale-distributors to re-import prescription drugs from Canada into the United States for resale.

*Drug Importation Act of 2002 (H. R.5186)*

The “Drug Importation Act of 2002” (H.R. 5186) would allow pharmacists to re-import FDA approved drugs for resale in the United States. As stated earlier, re-importation can be another source of counterfeit introduction. Any bills encouraging this activity must also tackle this threat before advocating re-importation.

---

8 Reconnaissance International, 16 Apr, 2003
http://www.pharma-anticounterfeiting.info/
Notable Examples of Counterfeits\(^9\)
(From the Pharmaceutical Research and Manufacturers of America (PHRMA).)

**Hong Kong – 3TC:** The quality of the packaging and labeling was remarkably good.

The counterfeiters even attempted to reproduce the covert anti-counterfeiting feature.

Counterfeit  
Original

**Malaysia - Viagra:** The counterfeits are excellent duplicates of the real. The counterfeiters replicated the Pfizer logo, blister card, foil backing and hologram!

U.K \ Taiwan – Zantac: This counterfeit product, manufactured in Taiwan and discovered in the United Kingdom, demonstrates the cross border threat of counterfeiting.

U.K \ India – Dermovate: On analysis, this product was found to be dangerous for use on human skin!
What Gets Counterfeited

The WHO reports that the majority of counterfeit cases involve tablets and capsules.

Antibiotics account for almost half of the reported cases of counterfeit drugs\textsuperscript{10}. The largest number of reports relate to antibiotics, anti-protozoals, hormones and steroids. In developing counties, antibiotics and other anti-protozoals such as anti-malarial drugs are commonly counterfeited. In developed countries hormones and steroids account for the majority of the cases reported. Generally, high volume (high consumption) and expensive drugs are the main targets of counterfeiters.

\textit{Classes of drugs reported as counterfeit from 2000 through 2001 (WHO)}

\begin{table}[h]
\centering
\begin{tabular}{|l|c|}
\hline
\textbf{Drug Type} & \textbf{Pct.} \\
\hline
Antibiotics & 28\% \\
Antihistamines & 17\% \\
Hormones & 12\% \\
Steroids & 10\% \\
Vasodilators & 7\% \\
Erectile Dysfunction & 5\% \\
Anti - Epileptics & 2\% \\
Other & 19\% \\
\hline
\end{tabular}
\end{table}

\textit{Types of tampering reported from 2000 through 2001 (WHO)}\textsuperscript{11}

\begin{table}[h]
\centering
\begin{tabular}{|l|c|}
\hline
\textbf{Tamper Type} & \textbf{Pct} \\
\hline
No Active Ingredient & 43\% \\
Poor Quality & 24\% \\
Low Content & 21\% \\
Wrong Ingredient & 7\% \\
Wrong Packaging & 5\% \\
\hline
\end{tabular}
\end{table}

\textsuperscript{10} World Health Organization, 17 Apr. 2003.
\textsuperscript{11} http://www.who.int/medicines/organization/qsm/activities/qualityassurance/counterfeit/counterfeit_info_facts.shtml

**Recent Counterfeit Incidences Compiled by the International Chamber of Commerce**

<table>
<thead>
<tr>
<th>Year</th>
<th>Country</th>
<th>Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>1990</td>
<td>Nigeria</td>
<td>109 children die after taking fake pharmaceutical preparation containing diethylene glycol</td>
</tr>
<tr>
<td>1991</td>
<td>Malaysia</td>
<td>Traditional aphrodisiacs and tonics mixed with the highly potent steroid Dexamethasone</td>
</tr>
<tr>
<td>1992</td>
<td>Bangladesh</td>
<td>Liquid paracetamol containing diethylene glycol believed to have killed hundreds of children</td>
</tr>
<tr>
<td>1993</td>
<td>China</td>
<td>Counterfeiter executed after giving fake medical injections leading to the deaths of three children</td>
</tr>
<tr>
<td>1996</td>
<td>China</td>
<td>Herbal remedies containing sand, flour and narcotics cause illness and deaths</td>
</tr>
<tr>
<td>1996</td>
<td>Haiti</td>
<td>30 children die after taking Afebril and Valodon which was laced with diethylene glycol</td>
</tr>
<tr>
<td>1996</td>
<td>Australia</td>
<td>Counterfeit steroids users visit clinics to get syringes and needles with added risk of contracting HIV and Hepatitis</td>
</tr>
<tr>
<td>1996</td>
<td>Niger</td>
<td>Fake meningitis vaccine leads to 3,000 deaths</td>
</tr>
<tr>
<td>1997</td>
<td>Vietnam</td>
<td>27 deaths caused by fake medicines</td>
</tr>
<tr>
<td>1998</td>
<td>Uganda</td>
<td>60% of all malaria deaths attributed to fake sugar-coated quinine sulphate</td>
</tr>
<tr>
<td>2000</td>
<td>Cambodia</td>
<td>30 people died after taking fake malaria drugs being sold as Mefloquine and Artesunate</td>
</tr>
<tr>
<td>2001</td>
<td>Indonesia</td>
<td>Many unwell after taking fake antibiotic capsules – DeryClin, Recomycin and Tetracycline</td>
</tr>
<tr>
<td>2001</td>
<td>USA</td>
<td>Amgen report that counterfeit Neupogen containing no active ingredient was in circulation in the US</td>
</tr>
<tr>
<td>2001</td>
<td>USA</td>
<td>Serono report discovery of fake Serostim</td>
</tr>
<tr>
<td>2002</td>
<td>USA</td>
<td>Tampered Zprexa, relabelled Epogen and Combivir and fake Serostim reported</td>
</tr>
</tbody>
</table>

**Counterfeit Products Reported In US During 2001 – 2003 from FDA MedWatch**

2001: Neupogen, Serostim, Nutropin AQ  
2002: Procrit, Epogen, Serostim, Combivir  
2003: Procrit

---

12 Reconnaissance International, 16 Apr, 2003  
http://www.pharma-anticounterfeiting.info/  
Compiled March 2003
Incidence of Counterfeiting Reported by the HDMA

- A 1993 magazine article reported that a counterfeit version of the ulcer medication Tagamet found to contain aspirin -- caused a woman's ulcer to bleed and develop a dangerous infection. A counterfeit of the antibiotic Ceclor caused children in seven states to suffer painful ear infections and risk possible ear damage because they received the wrong treatment.

- Another report indicates a patient purchased a 20-gm tube of Retin-A in Mexico for $2. Except for the ink color, the packaging was identical to the product sold in the U.S. for $20. However, the Mexican version of the powerful skin medicine was a counterfeit containing only vitamin A cream.

- The FDA recalled $7 million worth of intra-aortic pumps used during open-heart surgery, after it discovered malfunctioning counterfeit parts in the devices.

- In 1981, the pharmaceutical company Searle discovered that over 1 million counterfeit birth control pills had been distributed to unsuspecting women, resulting in unwanted pregnancies and irregular bleeding.

Industry Response

The industry has attempted to combat counterfeits in the past through a number of different techniques, but no method has yet proved adequate. Primarily, this is a result of not having the technology or the manpower to implement proper levels of inspection. The efforts that have been tried to date have relied on manual product inspection to check for counterfeiting. In the absence of automated inspection technology, this is too costly to do on anything more than a small sample of the total products been sold.
• Some drug companies have injected a chemical signature into their medications, which can be checked with a small handheld device much like a home pregnancy test (U.S. News & World Reports, 6/11/01).

• Tamper proof packaging, as well as technical measures such as holograms and difficult to replicate packaging designs and fonts have been used.

• FDA Medwatch (www.fda.gov/medwatch/index.html) is an excellent resource for patient safety information, from label changes to counterfeit product warnings and recalls.

• HDMA Product Safety Task Force (www.healthcaredistribution.org) strives to recommend steps and guidelines the industry should consider for the safe purchase of products.

• The Institute for Safe Medication Practices (www.ismp.org) is dedicated to the safe use of medications through improvements in drug distribution, naming, packaging, labeling, and delivery system design.

• Product Surety (www.productsurety.org) is a joint industry initiative with the FDA to curb the incidence of counterfeiting.

**A Solution to the Problem**

There is no single magic bullet to the problem of counterfeiting. A combination of strengthening existing techniques and using new technologies though, offers the possibility of significant reduction of counterfeits within the domestic supply chain over the next ten years. RF-ID technology, embedded within unit-of-use level packaging, is the key new technology this thesis will recommend for adoption in the battle against
counterfeiting. The ability to automatically track packaging, in real-time, will validate authenticity of products at any point in the supply chain. This technology, in conjunction with stronger legal enforcement and the use of existing technical countermeasures can radically alter the balance of power back into the hands of the pharmaceutical industry and away from the counterfeiters. This later group thrives on the anonymity of operation that is a result of the absence of tracking capabilities today. The following sections of this document will provide a more in depth analysis of the recommended solution.

**Methodology**

The methodology used to develop the ideas presented in this document includes literature reviews, interviews with industry participants, discussions with providers of counterfeit countermeasures, and cooperation from MIT’s Auto-ID center. Due to the still developing awareness of the problem of counterfeit within the industry, detailed information was often unavailable. However, many of the ideas presented in this thesis have met with initial support from industry participants as an approach that may be feasible for the industry to minimize the incidence of counterfeits. It should be noted, much of the information in this thesis came from interviews with industry officials who asked to remain anonymous.
II. Existing Non-RFID Based Anti-Counterfeit Technologies

Introduction

The pharmaceutical industry is beginning to realize the full impact of counterfeit products within their supply chain. While counterfeit has long been a problem in the developing world, it has only recently come to the forefront in the United States and Europe. Counterfeiting in the developing world, while pervasive, is difficult to control with technology because the attendant infrastructure does not exist to perform the necessary inspections of anti-counterfeit control mechanisms across such a complicated supply chain\textsuperscript{13}. For example, many drugs carry a bar code on them to indicate authenticity but most Indian apothecaries do not have bar code scanners\textsuperscript{14}. Therefore a cheap forgery that passes visually as a bar code is enough to escape detection. In these countries, legal enforcement is perhaps the most effective way to combat counterfeits. The cost of greater policing of distributors and retailers would also be great. The cost of a police force, though, is easier to share across the citizenry, while small distributors and resellers must purchase expensive technical solutions. Tax funds could be used to help these small players make these purchases, but then enforcement related funding would still be required to ensure that these funds were actually used for infrastructure upgrades and not other activities!

In the developed world though, anti-counterfeit technologies can be deployed to significantly curtail the occurrence of counterfeiting by increasing the entry barrier – i.e.,

\textsuperscript{13} Burns, Lawton. \textit{The Health Care Value Chain}. 2002.
the cost of equipment needed to produce passable replications. Yet even here, in the absence of push technology that actively communicates the occurrence of tampering to the owner, the labor costs of checking individual containers for counterfeit becomes prohibitively high. Additionally, even providing free high technology equipment to manufacturers in developing countries has possible drawbacks. The older technology that these manufacturers currently own, can find its way into the hands of counterfeiters at rock bottom prices. This reduces the overall cost of operations for counterfeiters and provides an entry point for illegal operations that may not have gotten of the ground otherwise. Due these sorts of challenges, anti-counterfeit measures have not yet found wide adoption. This study proves that these measures, in conjunction with an embedded RF-ID option, would present a far stronger deterrence to counterfeiting than present today.

Types of Anti-Counterfeit Technologies

Anti-Counterfeit technologies can be broadly categorized as covert or overt, and intra-formulary or package based. The industry, understandably, does not want to reveal details about most of these techniques, as this would benefit the counterfeiters. Pharmaceutical companies are reluctant to reveal information about covert technologies in particular. There are, however, a large number of these technologies. Unfortunately, this range of choices is itself an enabler for counterfeiting. It becomes a significant challenge for retailers or consumers to be able to keep track of exactly which anti-counterfeit technology to look for on a given version of a pharmaceutical. Therefore, a

15 Robin Koh, MIT Auto-ID Center, Interview, 1 May 2003.
counterfeit knows their odds of detection are lower. In addition, with manufacturers trying so many different strategies, counterfeiters have more likelihood of finding cheap substitutes for at least one of the technologies. As in any supply chain, the pharmaceutical chain is only as strong as the weakest link. Still, existing technologies do provide a measure of protection against counterfeits. What follows is a brief overview of some of the publicly available information about these methods.

**Overt Technologies**

Overt technologies like holograms and OVD (optical variable devices) are ones that aid consumers in detecting fraudulent product, as well as supply chain players. By imposing high cost, difficult to replicate, overt, anti-counterfeit measures manufacturers attempt to both minimize the number of people capable of producing a forgery and signaling brand authenticity to the end consumer. Of course the drawback to an overt measure is the possibility of creating a false sense of security to the consumer. Cheap knock-offs of otherwise expensive overt measures, like a fake hologram, can easily fool consumers into thinking they are buying legitimate product. In fact, studies have shown that even industry professionals and inspectors often fail to notice the differences between counterfeit packaging and authentic\(^{17}\). This problem has notably occurred for Procrit, which has had counterfeit versions sold undetected despite imperfect replication of overt countermeasures. Even in instances where trained inspectors are able to detect forgeries, the costs of labor-intensive visual inspection regimes are perhaps too high to ensure authenticity at the unit-of-use level.

**Covert Technologies**

Covert technologies, like invisible ink, present an additional barrier for counterfeiterers in that they must first ascertain that this measure has been taken and then attempt to uncover what measure it is exactly before they can attempt to replicate it. Covert measures, by their very nature, are unable to provide end consumers with assurance of authenticity. Like overt techniques, existing covert measures also share the same drawback on the cost of inspection. Not only do covert techniques require inspectors to have special testing kits to investigate authenticity, they also require validating organizations to have a full and current list of each covert technique employed per product type, per manufacturer, for today and for past items still in circulation. This latter requirement alone would become a staggering challenge for supply chain participants. There are third party organizations that provide inspection services to pharmaceuticals but even these organizations do not have the wherewithal to conduct unit-of-use level testing at every interchange of the product. Instead they rely on testing samples of highly counterfeit prone products. For example, counterfeit product tends to be more pervasive in the United States near the Mexican and Canadian borders so more sampling is done there. Similarly, high priced or high demand medicines are more likely to be counterfeited, so these are more rigorously inspected.

Anti-counterfeit techniques can also be categorized by where they are implemented. Measures taken within the actual dosage medication consumable are described here under Intra-Formulary Techniques. Measures taken on external packaging are described here under Package Level Techniques. Both of these techniques have covert and overt level implementations as described below.
Intra-Formulation Techniques

These techniques require the introduction of chemical additives in order to make medication more difficult to replicate. Once significant challenge facing this category of anti-counterfeit measures is regulatory approval and manufacturer trust. Any chemical additives to a pharmaceutical product must undergo rigorous stability testing before receiving FDA approval. Even after this hurdle has been achieved, independent manufacturers must be willing to accept these new formulations against the risk of reducing the efficacy of their product. In addition, these techniques do not lend themselves to visual inspection, and thus would incur substantial costs in any thorough inspection regime. For these reasons, one industry insider estimates that no more than 15% of the pharmaceutical industry has adopted intra-formulary methods as part of their anti-counterfeit programs.

Immunosassay

This covert technology involves the introduction of chemical additives during the formulation of individual medicines. The additive content is very low, on the order of a few parts per billion. The chemical compounds used are unique and kept secret. The only way to determine what compounds are used, in an effort to make unauthorized replications, would require the use of expensive techniques like high performance liquid chromatography. In some cases, even these methods would not be able to ascertain the molecular composition because so little of the marker is in the medicine. Once in the medicine, the testing procedure for authentication is simple. For example, one or two
drops of liquid medicine can be dropped on a low cost testing kit. The kit will show one line for authentic and two for counterfeit, much like a home pregnancy test kit. This technology, despite affordable costs for the additives and test kits, suffers from the drawback that inspectors must manually test individual pills. As a result, systemic testing is not possible with this method alone.

**Flavor**

In a few rare cases it is possible to create a special flavoring for a drug that is otherwise difficult to formulate. For example, it may be very difficult to formulate a banana flavor for a particularly bitter drug. The manufacturer’s special ability to introduce this flavoring constitutes a unique kind of overt anti-counterfeit measure. Of course, there is a severe problem with this implementation choice – a consumer must first consume the drug before realizing the fake. In most cases, consuming a counterfeit is not harmful to the patient, but in some cases it can be damaging. In addition, flavor determination won’t be possible when the product is consumed by the very young or the severely incapacitated.

---

Package Level Techniques

Package based techniques are the most prolific of anti-counterfeit measures. The wide range of methods available, and the relatively low cost of these techniques, allows organizations to deploy multiple package-based countermeasures on a single container in many cases. Companies combine overt and covert techniques on their containers to provide consumer recognizable authenticity as well as providing enhanced security due to the greater difficulty of detecting and replicating covert techniques.

Design

Design based countermeasures can be implemented either through the design of the package itself or by graphic design on the container. Package design can be crafted inside and outside the container, allowing for overt and covert implementations. The use of unique shapes and special die cutting to produce these packages can be cost effective for a large manufacturer due to the large volumes they produce. In contrast, counterfeit operations have difficulty in supporting such a large cost structure because the scale of their operations is so much smaller. But an industry insider opines that the growing sophistication of counterfeiting operations has often made package based techniques easy to replicate.

Graphic design changes, typically much lower in cost, are often implemented by creating patterns using shapes instead of the usual dot-based techniques that most printers use. These designs are generated by software that utilizes shapes, relief work, anti-copy non-reproductive backgrounds and patterns, and micro-text to create hard to replicate
images. Most counterfeits use simple scanning technology to replicate designs. These security-enhanced graphics appear distorted or muddy when scanned. Of course, more expensive replication techniques can be used in order to circumvent these tactics.

Another graphic technique is to make intentional errors within embedded micro-text like a reversed letter or dropped punctuation. Counterfeiters will often fail to spot these minute differences and thus make flawed replicas. As other visual inspection based methods though, detection of micro-text replication flaws requires significant scrutiny and thus is a labor-intensive process.

**Watermarks**

Watermarking technology, which incorporates images onto paper that is visible only when held up to light, is most famous as a currency anti-counterfeit measure. This traditional watermark technology has not been successful as a countermeasure in the pharmaceutical industry. Digital watermarks, not yet in wide use, hold more hope to foil would-be forgers. These watermarks utilize readers attached to computers to “read” the hidden embedded images/data. The requirement of a reader though, adds significantly to the cost. There is also a patented watermark technology that encodes graphics visible with merely a simple plastic lens. This technique is more popular than the traditional latent image (a hidden image that appears when the document is tilted) watermark in that it can be created with more standard packaging printing processes. The latent image technique only works with intaglio printing, an engraving technique typically used in currency printing. In contrast, digital design technologies can be printed using the offset,
flexo, gravure, and digital printing methods common to pharmaceutical packaging. But this method too suffers the same drawback of requiring visual inspection of some kind to verify authenticity.

**Fibers and Threads**

This technique is implemented by integrating threads or fibers that can be holographic, fluorescent, metalized, magnetic, or diachronic optically variable (changes with time). These techniques, like most other anti-counterfeit measures, can be varied by region to trace diversion in addition to counterfeit. The security threads can be incorporated into tear strip for packaging, providing the dual role of authentication and tamper evidence. Combinations of embedded fibers can even be used to uniquely identify individual containers to provide track and trace capabilities. Magnetic threads can be incorporated as a covert protection method. This application though is a relatively high cost solution.

**Reactive Inks**

There are a wide variety of ink technologies used in anti-counterfeit technology. They vary can vary greatly in cost, usage level, and level of security. One low priced option is chemically reactive inks. These inks are reactive to various chemical treatments. Solvent sensitive inks are sensitive to certain solvent mixtures. Because of the destructive nature of this test, it is limited to tamper evident feature applications. One technology that allows authentication without destruction is reactive inks that reversibly changer color when treated with specific chemicals like ammonia.
Heat sensitive inks contain dyes or pigments that change color when subjected to high temperatures. These inks have wide spread usage because they are low in cost, non-destructive, and easy to test. Pressure sensitive inks are similar in that images form when subjected to external pressure. Photochromic inks will temporarily change color when exposed to ultra-violet light. Unfortunately, photochromic inks lose their efficacy if subjected to prolonged exposure to daylight. A similar technology is the use of infrared inks. These inks emit infrared light upon excitation by higher energy light (such as visible light). These inks provide a covert countermeasure because they require an IR reader for detection and are moderately priced. Perhaps the most secure of reactive ink-based solutions is the optically variable ink family. These relatively new compounds shift color when viewed at different angles. This overt technique is so secure because they are considered nearly impossible to counterfeit. In addition, despite being priced similar holographic techniques, they do not require hot stamping or label application like the latter.

**Holographic (OVD)**

Holograms are the most popular kind of optically variable devices (OVD). They are also the most pervasive anti-counterfeit technology in use worldwide (including non-pharmaceutical industries). Pigments, and inks (as mentioned previously) are other kinds of optically variable technology. Holograms can be directly hot stamped onto a package or applied with pressure sensitive labels. Cost estimates for holographic technology hover around $.02 to $.05 per hologram, including the cost of application. Unfortunately, the counterfeit industry has proved very effective in faking holograms. One industry expert
saying that in Asia, where hologram counterfeiting is particularly pervasive, forgers produce relatively accurate replications within days of the original packaging.

*Numeric – Bar Code*

Bar coding is another technique used both for track and trace and as a counterfeit countermeasure. Bar code implementations require line of sight readers in order to scan and verify a bar code. This technology is in widespread usage already within the United States and Europe. But in countries where this infrastructure is not yet available, bar code countermeasures offer no additional security. Forgers in these countries apply fake bar codes onto packaging and without bar code readers to verify authenticity, easily escape detection. Bar coding infrastructure, having been around for over twenty-five years now, has become relatively inexpensive. Its cost of about $.01 cent per label is the target price for all new similar technologies. Despite this low price point, a consideration not often included in the cost analysis is the significant cost of bar code scanning. The line of sight readers required to scan a bar code require close individual inspection. The true cost per bar code label then is significantly higher than the oft-quoted $.01 price tag.
III. Overview of RFID Technology

Introduction

(Quoted text below taken from a related RF-ID article by Mark Denning of Dell and Edmund W. Schuster)

“Currently under development at MIT, Auto-ID technology holds great promise to solve age-old problems in material control through the application of low-cost, Radio Frequency Identification (RFID) tags. By placing RFID tags on individual items, cases and pallets, along with readers at strategic points within the supply chain, Auto-ID technology will provide instant two-way communication by merging information with physical goods. Auto-ID technology also incorporates the Internet as a means of transmitting data gathered from RFID tags, combined with a new communication protocol called PML (Physical markup language).

RFID technology has been in use for approximately thirty years in the defense and transportation industries, where “active” RFID tags and proprietary systems are in place. Most of these applications involve different types of capital asset tracking and management. For example, rail cars and steamship containers are tracked through switching rail yards and holding terminals at ports. Each active tag requires a small battery that provides electric power to generate and transmit the radio frequency signal. Active tags can be read from a relatively long range—up to 30 meters. However, the greater the scanning distance, the greater the chance of a “frequency collision.” Also, with longer read distances, the opportunity of providing exact location information diminishes. The tiny batteries are moreover somewhat expensive, thus limiting
widespread use. Common prices for active tags range from $2 or more per unit, depending on capability and order size.

Since 1999, MIT has conducted research to drastically reduce the cost of Auto-ID technology through the use of “passive” tags. With this technology, each tag does not contain a battery. Rather, the energy needed to power the tag is drawn from electromagnetic fields created by readers that also serve a dual purpose of gathering the signals emanating from the passive tags. Since no fixed power source is required, passive tags hold a great advantage over active tags in terms of lower cost per unit. This opens the possibility for the use of passive tags in a far greater number of applications. Gradually, as costs decrease, passive tags will selectively replace bar codes as a means of gathering information within supply chains. The goal is to produce a passive tag for less than 5 cents per unit. At this cost, passive tags are feasible for widespread application within a number of industries, including high volume consumer goods manufacturing. Items such as razor blades, batteries and perfume, all with high selling prices, are excellent candidates to utilize passive RFID tags for inventory control and theft prevention.

The MIT Auto-ID Center currently has financial support from 83 leading manufacturing and technology/equipment firms to research, develop and test passive tags for a number of RFID applications. Field test results completed during winter 2002, involving Wal-Mart, Proctor & Gamble, Gillette and Unilever, demonstrated that passive tags, along with the Internet infrastructure to handle data, worked as envisioned. These field tests dealt with pallet and case
identification; however, other tests have shown that passive tags applied to individual items on store shelves also can be successfully read under laboratory conditions. Ongoing efforts involving more intensive field tests are planned for 2003 and will include scanning of tags placed on individual items made of metal or containing liquids. In summary, passive RFID works. Though the economics of passive tags are not fully understood at this time, the future looks bright for application of this technology to improve supply chain performance.”

As this synopsis of RF-ID technology suggests the potential for RF technology is just beginning to be tapped. This thesis advocates that passive tag systems be extended into the pharmaceutical supply chain in addition to the areas where it has already been tried. While the technology is ready to use today, considerable work remains to be done in order to define the business rules that will govern this new intelligent supply chain. The first step is to get a rough sense of what the cost-benefit analysis for this technology looks like. The following section outlines a preliminary attempt to capture these costs and benefits.
Rough Cost Estimate for One Possible RF-ID Implementation

The following spreadsheet outlines the cost of an RF-ID implementation for one manufacturer. It is based on an assumption of selling one hundred million unit-of-use level products in one year. Company revenue is set at 2.5 billion dollars for this product. The estimates are a very rough estimation meant to help delineate the relevant components that need to be analyzed for a total cost of ownership study. In addition, RF related costs are based on high-volume production of tags and readers.

Cost Estimate for First Year RF Implementation for Manufacturer

<table>
<thead>
<tr>
<th>Unit of Use Level RF-ID Scenario</th>
<th>Yearly</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Definition</td>
<td></td>
<td>Assumption: Blue questions require user input, Bold indicates calculations</td>
</tr>
<tr>
<td>Yearly Company Revenue</td>
<td>$2,500,000,000</td>
<td>Results for last year</td>
</tr>
<tr>
<td>Number of SKU</td>
<td>1,000</td>
<td>How many different products are sold</td>
</tr>
<tr>
<td>Items per SKU</td>
<td>100,000</td>
<td>How many items per product are sold</td>
</tr>
<tr>
<td>Total Item Count</td>
<td>100,000,000</td>
<td>Total items sold per year</td>
</tr>
<tr>
<td>Items per Level 1 Aggregation</td>
<td>100</td>
<td>How many items per box/drum or initial bundling level</td>
</tr>
<tr>
<td>Items per Level 2 Aggregation</td>
<td>50</td>
<td>How many items per pallet or secondary bundling level</td>
</tr>
<tr>
<td>Total Aggregator eTags</td>
<td>1,020,000</td>
<td>How many tags needed to mark box, pallets, etc.</td>
</tr>
<tr>
<td>Total eTags</td>
<td>101,020,000</td>
<td>How many total tags needed for year</td>
</tr>
<tr>
<td>Inventory Turns per Year</td>
<td></td>
<td>How much of total item count can be expected to be in inventory 3at a given time</td>
</tr>
<tr>
<td>Total Tags Needed per Period</td>
<td>33,673,333</td>
<td>Period is time needed for 1 inventory turn</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>eTag Infrastructure</th>
<th>Assumption: Costs based on mass production of eTags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price per eTag</td>
<td>$0.05PASSIVE RF-ID tag with antennae</td>
</tr>
<tr>
<td>Price per Agile Reader</td>
<td>$250Reader supporting multi-frequency tags</td>
</tr>
<tr>
<td>Reader Maintenance (%)</td>
<td>20%* indicates on-going cost. Yearly cost for reader maintenance.</td>
</tr>
<tr>
<td>eTags per Reader</td>
<td>1,000 How many STATIC tags a Reader can talk to w/o overload</td>
</tr>
<tr>
<td>Readers per Savant Server</td>
<td>50 Number of savant servers needed to support all readers</td>
</tr>
<tr>
<td>One Time Price for Savant Software</td>
<td>$100,000Includes Savant and PML related code NOT integration to ERP</td>
</tr>
<tr>
<td>One Time Price for Savant Hardware</td>
<td>$5,000Cost for server.</td>
</tr>
<tr>
<td>One Time Cost to Install eTag Systems</td>
<td>$1,000,000Estimated cost to install eTag embedding equipment</td>
</tr>
<tr>
<td>Cost per 1000 eTag installations</td>
<td>$0.10Estimated cost to install eTag on packages</td>
</tr>
<tr>
<td>Number of Readers Needed</td>
<td>33,673Number of readers needed to read all tags</td>
</tr>
<tr>
<td>Number of Savant Servers Needed</td>
<td>673Number of Savant servers needed for readers</td>
</tr>
<tr>
<td>Cost for eTag purchase*</td>
<td>$5,051,000Yearly cost to buy eTags</td>
</tr>
<tr>
<td>Cost for eTag installation*</td>
<td>$10,102Yearly cost to install eTags onto packaging</td>
</tr>
<tr>
<td>One Time Cost for eTag Systems Install</td>
<td>$1,100,000One time cost to install eTag related systems</td>
</tr>
<tr>
<td>One Time Cost for Readers</td>
<td>$8,418,333ONE TIME cost to buy reader infrastructure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT Specific Infrastructure</th>
<th>Assumption: Vendor stores all personal tag info locally. Avg tag life is 1 year.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descriptor File Size per eTag (MB)</td>
<td>48 Storage space needed to archive tag data</td>
</tr>
<tr>
<td>Storage for Descriptor Files (TB)</td>
<td>48 Storage space needed to ensure high uptime</td>
</tr>
<tr>
<td>Redundant On-Line Storage (TB)</td>
<td></td>
</tr>
<tr>
<td>Cost per TB of SAN Storage</td>
<td>$25,000 Generic price for EMC SAN</td>
</tr>
<tr>
<td>Cost for High Transaction Database</td>
<td>$150,000 Oracle DB with failover support for high uptime</td>
</tr>
<tr>
<td>Cost for Presentation Layer Software</td>
<td>$150,000 Web Server, App Server, Middleware</td>
</tr>
<tr>
<td>Software Maintenance (%)</td>
<td>20% Yearly charge for maintenance</td>
</tr>
<tr>
<td>Cost for Software Maintenance*</td>
<td>$60,000 On-going cost for maintenance</td>
</tr>
<tr>
<td>Cost for Software Installation Services</td>
<td>$250,000 Cost to install database infrastructure</td>
</tr>
<tr>
<td>Cost for ERP Integration Services</td>
<td>$250,000 Cost to integrate eTag information into existing data repositories</td>
</tr>
<tr>
<td>Cost per TB of Backup Data</td>
<td>$5,000 Cost to do nightly incremental backup of tag data to tape</td>
</tr>
<tr>
<td>Cost for Servers</td>
<td>$125,000 Assumess 5 large servers to run all software</td>
</tr>
<tr>
<td>Hardware Maintenance (%)</td>
<td>15% Yearly charge for maintenance</td>
</tr>
<tr>
<td>Cost for Hardware Maintenance*</td>
<td>$18,750 On-going cost for maintenance</td>
</tr>
</tbody>
</table>

| Total Cost for Storage*          | $2,408,504 Cost to buy SAN storage                                             |
| Total Cost for Software+Services | $550,000 Cost for all eTag software, services                                |
| Total Cost for Backup*           | $240,850 Cost for nightly backups                                             |
| Total Cost for Hardware          | $125,000 Cost for servers                                                     |
| Total Cost for Maintenance*      | $78,750 Cost for Software and Hardware Maintenance                            |

| Total Startup Costs for DB Infra. | $675,000 IT Startup                                                          |
| Total Recurring Costs for DB Infra. | $2,728,105 IT Recurr.                                                      |
| Total Cost for DB Infra. For Year One | $3,403,105 Total Cost for all IT infrastructure                             |

<table>
<thead>
<tr>
<th>Summary of Expenditures</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup Costs</td>
<td>$13,560,667</td>
</tr>
<tr>
<td>Recurring Costs</td>
<td>$10,146,340</td>
</tr>
<tr>
<td>Total Costs for Year One</td>
<td>$23,707,007</td>
</tr>
</tbody>
</table>

| Startup Cost Percent of Solution | 57%                              |
| Recurring Cost Percent of Solution | 43%                             |
| eTag Cost Percent of Sales       | 0.9%                            |
Summary of Costs by Recurring and Startup by Percentage

Breakdown of Costs

5%  20%  33%  42%

- eTag Startup
- eTag Recurr.
- IT Startup
- IT Recurr.
Cost Benefit Analysis

The costs associated with RF-enablement are high, but the benefits ultimately justify the expenditure. Certainly the value of saving lives is incalculable, but even more concrete measures can be used to justify the expenditure. The table below provides a justification based on tangible benefits of recovering revenue lost today to counterfeiting. The numbers are rounded estimates from the analysis above. Critical assumptions as explained after the table.

Cost Justification for RF Technology Adoption

<table>
<thead>
<tr>
<th>Feature</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Yearly Revenue</td>
<td>$2.5 Billion</td>
</tr>
<tr>
<td>Pct Loss Due to Counterfeit</td>
<td>5 %</td>
</tr>
<tr>
<td>Revenue Lost to Counterfeit</td>
<td>$125 Million</td>
</tr>
<tr>
<td>Number of Units Sold Yearly</td>
<td>100 Million</td>
</tr>
<tr>
<td>Number of $100 Readers Needed</td>
<td>33,000 Units</td>
</tr>
<tr>
<td>Total eTags Needed</td>
<td>35 Million</td>
</tr>
<tr>
<td>Total Fixed Cost</td>
<td>$13.5 Million</td>
</tr>
<tr>
<td>Total Recurring Cost (20% Maint.)</td>
<td>$10 Million</td>
</tr>
<tr>
<td>Yrly Benefit (50% Fraud Detection)</td>
<td>$50 Million</td>
</tr>
</tbody>
</table>
The cost justification table makes the following assumptions:

1) 5% of manufacturer revenue is lost through counterfeit sales of their product (WHO estimates 5%-7%).

2) Number of units sold and readers based on calculations from the table on cost estimates.

3) Fixed costs include the cost of the readers and startup cost for IT infrastructure.

4) Yearly benefit is based on 50% reduction of counterfeits due to RF technology. Benefit is calculated using recurring cost, not fixed cost because the later is paid out only during the first year. With these calculations, even a 10% reduction in counterfeit would provide breakeven on costs.

5) Other tangible benefits like inventory reduction and better supply chain management are not factored in this analysis.
Comparison of Anti-Counterfeit Technologies

Described below is a list of existing anti-counterfeit measures, with an explanation of use, likelihood of replication, and price. It is not meant to be an exhaustive list but does contain the chief measures being taken today. One industry expert believes only about one-half of pharmaceutical manufacturers are estimated to have adopted any of these techniques, but adoption level is expected to grow.

<table>
<thead>
<tr>
<th>Anti-Counterfeit Measure</th>
<th>Type</th>
<th>Type of Inspection</th>
<th>Likelihood of Replication</th>
<th>Price</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intra-Formulation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Immunoassay</td>
<td>Covert</td>
<td>Chemical</td>
<td>Low</td>
<td>Med</td>
<td>Difficult FDA approval</td>
</tr>
<tr>
<td>Unique Flavoring</td>
<td>Overt</td>
<td>Consumption</td>
<td>Low</td>
<td>High</td>
<td>Infrequent applicability</td>
</tr>
<tr>
<td><strong>Package Level</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design</td>
<td>Overt</td>
<td>Visual</td>
<td>High</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Watermarks</td>
<td>Both</td>
<td>Visual, Reader</td>
<td>High</td>
<td>Low</td>
<td>Limited print processing options</td>
</tr>
<tr>
<td>Digital Watermarks</td>
<td>Both</td>
<td>Reader</td>
<td>Low</td>
<td>Med</td>
<td>Still new method</td>
</tr>
<tr>
<td>Fibers and Threads</td>
<td>Both</td>
<td>Visual, Reader</td>
<td>Med</td>
<td>Med</td>
<td></td>
</tr>
<tr>
<td>Reactive Inks</td>
<td>Both</td>
<td>Visual, Chemical, Reader</td>
<td>Med</td>
<td>Med</td>
<td></td>
</tr>
<tr>
<td>Holograms, OVD</td>
<td>Both</td>
<td>Visual, Reader</td>
<td>High</td>
<td>Med</td>
<td></td>
</tr>
<tr>
<td>Bar Code</td>
<td>Overt</td>
<td>Reader</td>
<td>High</td>
<td>Low</td>
<td>Well established</td>
</tr>
<tr>
<td><strong>Active Technology</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFID</td>
<td>Covert</td>
<td>Automatic</td>
<td>Low</td>
<td>High</td>
<td>Early stages</td>
</tr>
</tbody>
</table>
IV. Preventing, Detecting, and Resolving Counterfeits

Overview of Solution

The proposed solution to more successful counterfeit prevention, detection, and resolution is comprised of five parts: legal changes, greater vigilance, supply chain cooperation, non-RF-ID based technical measures, and RF-ID measures. Without the successful implementation of all of these components the overall efficacy of anti-counterfeit measures will be weakened. This section outlines the first four. The next section outlines the final component in detail.

Legal Changes

Legal changes can be separated into two categories: industry regulation and punitive measures. The FDA and many state governments have numerous regulatory and punitive stipulations pending. The Federal government today governs the standards to which manufacturers must comply. State governments provide the controlling legislation over distributors. Among state governments, Florida has taken a lead in legislating tougher laws against counterfeitors\textsuperscript{20}. The Federal government though, has not been as quick to accept the threat of counterfeits\textsuperscript{21}. Recent bills have pushed to allow the re-importation of drugs, which are often sold more cheaply elsewhere, from abroad – a category of medicine particularly susceptible to counterfeiting\textsuperscript{22}. In addition, the recent federally sponsored Patient Safety bill, which seeks to better protect patients from medical malpractice, does not mention counterfeiting as a threat to patient safety. Clearly,

\textsuperscript{20} "Tighter Rules Urged on Fake Drugs", Miami Herald, 5\textsuperscript{th} March, 2003.
\textsuperscript{21} "Drug Reimportation Seen Continuing Despite Glaxo Move", Dow Jones News Wire, 13\textsuperscript{th} Jan 2003.
\textsuperscript{22} "Officials Say Patients Face Serious Risks From Counterfeit Drugs", Boston Globe, 27\textsuperscript{th} Aug, 2001.
fake medicines do constitute a threat to patient safety. For reasons such as this some anti-counterfeit advocates believe that the growing threat of domestic counterfeiting has outgrown the existing controlling legislation. This proposal will not attempt to assess pending legislation or decide whether new regulations should be mandated at the Federal or State level. Instead it will provide a general framework around which industry experts can determine specifics. But it is important to remember that any new actions taken are implemented with consideration for the business exigencies of pharmaceutical supply chain players. In addition, new legislation must strike a balance between tougher punishment of counterfeiters to act as a deterrence, and sentencing that provides for the possibility of rehabilitation.

**Industry Regulation**

> Government mandated industry regulation is needed to require large, U.S. based, prescription pharmaceutical supply chain partners to provide domestic product authentication for each unit-of-use level container at every exchange of ownership. In addition, the final organization selling a prescription drug to the consumer must be able to validate product authenticity at the point of sale. A large supply chain partner is defined here as one that earns yearly domestic revenues over $100 million dollars from selling prescription pharmaceuticals. Supply chain partners include manufacturers, distributors, retailers, returns handlers, transporters, and authentication firms. Products that U.S. based firms sell abroad are not covered by this proposed regulation once the product is shipped out of domestic ports. U.S. firms channeling their own products into America from foreign nations must begin validating authenticity from product entry into this country.
Non-American firms selling into this country are not restricted by this proposal at this time. For example, an American distributor buying from an American manufacturer would need to provide validation that upon receipt of the product each unit-of-use container was inspected for authenticity. But a non-American manufacturer could sell to an American distributor without providing unit-of-use level authentication. In this case, the American distributor would be the birth of the unit-of-level tracking. This scenario does not ensure authenticity of imported products. At this point, only ensuring the authenticity of products once they are inside the domestic supply chain is being addressed. Global coordination is ultimately needed, but the large amount of time needed to gain consensus on a global architecture requires that a domestic solution be implemented to begin with. Counterfeits pose a severe health risk to Americans, and detecting their occurrence within the domestic supply chain will still dramatically improve the quality of pharmaceuticals.

These regulations would apply only to the class of drugs most likely to be counterfeited – at this time this would include cancer and AIDS medicines, high cost prescription medicines and other drugs to be determined by the FDA. Due to the high capital costs and remaining technical hurdles for this endeavor, implementation should be phased in over a number of years. It is expected that smaller firms and international firms not subject to this regulation in this current proposal would ultimately be required to come into compliance as the technology became more pervasive.
The reason this action needs to be legally mandated, and not left to voluntary
adoption, is to prevent early adopter disadvantages accruing to firms that voluntarily
choose to implement the Auto-ID infrastructure first. Without a legal mandate, there is a
disincentive for initial adopters of this solution because they have no assurance that other
downstream players will implement the requisite technology needed to provide
authentication. In addition, early adopters will bear the higher initial costs of purchasing
new technology while later entrants would enjoy the benefits of buying these components
at the cheaper prices that mass production would provide. Finally, a lack of mandate
provides a perverse incentive for industry players to NOT take anti-counterfeit measures!
As long as the industry stays unaware of the true size of the problem and lacks the tools
to address it, they are not nearly as culpable for the damage. Therefore, the industry is
currently counter-incented from developing greater visibility into their supply chain.
These complications would serve to be inhibit the adoption of this solution, but can be
avoided if all players are mandated by law to implement this architecture simultaneously.

Another unrelated but important piece of regulation needed is to require supply
chain participants to notify all findings of counterfeit product to the FDA. The FDA will
judge when the information should be made public. This will ensure that detecting
obvious one-time counterfeits does not trigger a nation wide scare, while alerting patients
about possible problems with their medication in a timely manner. The current regime,
which allows organizations to choose when and whether to divulge the incidences of
counterfeit, violates a patients’ right to know about a product whose effects are ultimately
felt by him or her. The moral hazard attendant with this practice presents an unacceptable risk.

**Punitive Measures**

Industry experts universally agree that current laws against counterfeiting are too lax. Some familiar with the problem have noted that former traffickers in illegal narcotics have switched to pushing fake medicines because of the weaker laws and looser enforcement associated with the later. Existing laws need to be strengthened in relationship to the severity of the deception. The strongest punishments should be meted out to counterfeiters that substitute large quantities of life-saving medicines with drugless placebos and the weakest punishments to those that forge packaging as a means to divert product into inappropriate channels. Counterfeiting medicines sold primarily to the elderly should also face sterner sentences because this segment of the population is least able to visually inspect packaging due to the small lettering and design of most medical containers.

**Greater Vigilance**

**Supply Chain Members**

An important step needed to reduce the incidence on counterfeiting is greater vigilance and scrutiny of pharmaceutical supply chain members. Certainly the vast majority of these organizations are operating within the law, but the few that are not sully
the good name of the industry as a whole. Greater vigilance of distributors in particular is needed, as evinced by the recent findings in Florida\textsuperscript{23}.

In addition, like so many other American industries, the events of 9-11 also affect the pharmaceutical supply chain. It is imperative that we secure our critical supply of drugs from being infiltrated by future terrorists. Given the large amounts of financing available to the terror networks and their American presence, it would not be difficult for them to introduce visually accurate counterfeits into today’s supply chain.

**The FDA**

The FDA today has only has 175 full-time-equivalent employees assigned to the task of analyzing the entire supply of medicines in the domestic market and those coming in via importation. This is far too overwhelming a task for so few employees. In particular, a more widespread inspection regime needs to be mandated for medicines or medical ingredient being shipped into the United State\textsuperscript{24}. The WHO estimates that 8% of imports to the U.S. are counterfeit. Because it is not possible to authenticate many of these imports before they arrive to the States, it is imperative that they be subjected to greater scrutiny as they enter American borders. The FDA admits it has information on only 18 percent of the foreign drug manufacturers shipping to the U.S. One expert reports that since 1997, some 4,600 foreign drug makers have shipped medication into the U.S. without getting inspected.

\textsuperscript{23}“Florida’s Wholesale Drug Industry Has Been Corrupted, Jury Says”, South Florida Sun-Sentinel, 28\textsuperscript{th} Feb. 2003.

\textsuperscript{24}“US FDA Slammed Over Counterfeit Bulk Drugs”, Marketletter, 22\textsuperscript{nd} May 2000.
Police Force

Police forces across America need better training to be able to identify that the speeding car they have just stopped is full of counterfeits. In many cases today, lack of police awareness to this new threat allows forgers to slip literally out of the hands of enforcement officials. With RF-enabled tools, officers could immediately check any containers of medicine for authenticity by checking the product EPCs.

Medical Community

Medical professionals need also to be made aware of the possibility that patient morbidity may be a result of consuming fake medicines and not just indicative of resistance to the prescribed medicine. In many cases, patients taking counterfeits complain of product ineffectiveness to doctors and are told merely to take the medicine for longer periods, further exacerbating the problem. Earlier detection can result only once the problem of counterfeits is highlighted more strongly to the medical community.

Supply Chain Cooperation

One reason that counterfeiters find it increasingly easier to enter the American market is the lack of coordination among pharmaceutical supply chain partners. As the number of distributors multiply, it becomes easier for small operations to infiltrate the supply chain undetected. One way to counter this movement is for manufacturers, distributors, and retailers to integrate their supply chains more closely. This will allow them to more readily validate that the products they are handling are authentic. In addition, greater trust among supply chain partners is needed in order for the RF based
solution proposed here to be truly effective. In particular, some of the costs related to implementing an RF infrastructure should be treated as shared costs by the industry as a whole. All supply chain partners will benefit from a reduction in counterfeit products and therefore they should all work together to minimize the cost of the solution.

**Non RF-ID Based Technical Countermeasures**

Even in a scenario where all unit-of-use level medical packaging has intelligent embedded tags there is an important role to be played by other technical countermeasures. Due to current technical limitations, the RF tags cannot be embedded on individual pills or liquids. People may not like the metallic aftertaste of eating an RF microchip along with their medicine! Therefore, pill level authentication measures, like the intra-formulary techniques described previously will remain an important component of the overall solution. In addition, just because a package is being continuously tracked does not mean that it was not opened and its original contents replaced with adulterated versions. Therefore tamper evident packaging is also required. In some applications, the RF tag itself can be placed in the tamper evident foil and upon package opening, the destruction of the tag will be communicated to the manufacturer. Finally, non RF measures are particularly important in preventing counterfeits in supply chains that are not initially able to purchase RF related infrastructure. Therefore, in the initial rollout of the RF based solution, bar coding, packaging and other existing countermeasures are all expected to play a significant role in the fight against counterfeiting.
V. Using RF-ID as a Countermeasure

RF-ID as Counterfeit Prevention

Automated Authentication

Embedded, on-package, RF tags represent the biggest technological requirement of the proposal presented in this document. These RF tags though, also form the cornerstone for counterfeit prevention. Once each unit-of-use level package (package indicates bottle, blister pack, or whatever bundling level constitutes “unit-of-use” for a given drug) bears an embedded tag, this covert technology will allow real-time, location specific, monitoring of the medical supply chain. Most importantly, this track and trace mechanism is the only one able to communicate information about itself without human intervention. This automated authentication capability is the critical factor in reducing the cost of vigilance to a price point that allows for inspection at the unit level. The other technical solutions described earlier offer significant additional value, but ultimately fall short of providing true security. These technologies all require human intervention, either via visual inspection or through the use of special line of sight readers, in order to ascertain authenticity. This additional step limits these technologies from being cost effective at the unit level.

Difficulty of Replication

Another significant reason that RF technology is critical to this endeavor is the difficulty of creating unauthorized replicas. Other countermeasures like design and holograms have shown to be quickly countered with knock-off replicas. In contrast,
creating fake Electronic Product Codes would be nearly impossible. The manufacturers strictly control the supply of the tags and the EPCs. Engineering tags through an independent factory would be very challenging due to the technical sophistication of the product. In addition, each applied tag will contain a unique identifier, the EPC, that matches with the same code at the manufacturers sight. So if a new tag with a new identity were introduced, it would be spotted as non-existent during the first authentication read. Similarly, attempts to re-use or duplicate a tag would also send an alert to the original manufacturer that multiple, geographically disparate tags were in use.

**Overview of Proposed Solution Architecture**

The RF architecture is comprised of tag related hardware and software components as well as information management related hardware and software components. This document will outline an implementation scenario for only the latter. Information about tag related hardware and software (tags, agile readers, ONS, Savants, etc) can be found in documentation at www.autoidcenter.org. The AutoID related information management solution is comprised of three different types of databases whose access levels are restricted based on business rules defined by supply chain partners. The Manufacturer Database will contain static product information about the particular item. This data includes the product name, creation and expiry date, and perhaps offer a link to the Red Book or First Interstate catalogs which contain a registry of medical products and their images. The Audit Database will contain the trail of all exchanges of a product in the supply chain. Finally, the Local Database will contain product info local to an organization, like warehouse location and internal sign-offs.
Diagram of RF-enabled Supply Chain

Manufacturer Database

The most externally accessed of the three databases is the Manufacturer Database (MDb). This database will contain the static information about the product like its creation and expiry date, as well as usage instructions. This database will be the one accessed, via the Internet, by outside sources to authenticate the product, unless a Break Bulk Distributor creates a Distributor Database (DDb). This is an exceptional case where a distributor creates new unit-of-use level packaging for a medicine by breaking the original package into smaller packages for resale. When this is done, the distributor becomes the source for EPC authentication. All information about the EPC will be kept in an EPC specific record called the Descriptor File.
**Audit Database**

Another database needed for this solution is the Audit Database (ADb). The ADb will be maintained at a 3rd party site. This proposed site will be a joint venture of supply chain members and will be charged with retaining confidential audit trail information. No single supply chain member will have access to information about the exact channel path by which a particular medicine was sold. In the event of a counterfeit, recall or other such exceptional event, organizations such as the FDA may be privileged to see the full audit trail for ONLY the EPC in question. Supply chain members can grant privileges to organizations to view each other’s audit information on a case-by-case basis.

**Local Database**

Finally, there will also be a series of Local Databases (LDb). These databases will be resident at every supply chain partner who records information from the RF tag. This information will remain local to the organization. It will include information such as telemetric and environmental information, who did QA on the product, price of sale, and other such proprietary information.

These three tiers of databases will ensure that the privacy of supply chain members is protected while allowing a rapid means for authentication and problem resolution. Outlined below is a detailed explanation of the responsibilities incumbent of supply chain partners.
Manufacturer Components

Ingredients Suppliers

Suppliers of ingredients for the production of drugs will NOT be responsible for the creation of EPC tags. They will continue to use the track and trace mechanism they use today. Upon creation of the EPC by the Dosage Manufacturer, these internal tracking codes can be saved onto the new file.

Bulk Pharmaceutical Manufacturers

Bulk manufacturers of drugs will NOT be responsible for the creation of EPC tags. They will continue to use the track and trace mechanism they use today. Upon creation of the EPC by the Dosage Manufacturer, these internal tracking codes can be saved onto the new file.

Dosage Pharmaceutical Manufacturers

The manufacturers of dosage pharmaceuticals will generate the Manufacturer EPC tags. This tag will be the official tracking ID used by all downstream organizations, except in cases where there is a break bulk and new EPC tags are created (addressed later). The Manufacturer EPC will be generated during the batch production cycle. Immediately upon creation the of the EPC, a Descriptor File will be created containing the following set of information:

- Ingredient Information: Batch\Lot number of all ingredients used. Manufacturer, creation date, and expiry date of each ingredient. Verification of ingredient
efficacy where applicable. Quantity included. Status of product. Date sold to purchaser.

- **Bulk Manufacturer Information**: Batch\Lot number of all bulk drugs used. Manufacturer, creation date, and expiry date of each bulk pharmaceutical product used. Verification of product efficacy where applicable. Quantity included. Status of product. Date bought from seller. Date sold to purchaser.

- **Dosage Information**: Batch\Lot number of dosage production run. Manufacturer, creation date, and expiry date of drug. Verification of product efficacy where applicable. Quantity included. Status of product. Date bought from seller. Date sold to purchaser.

- **Link to Product Catalog**: A reference will be provided when possible to where a user can go to find the product catalog information about the medicine. This information is commonly provided by organizations like Red Book and First Interstate.

- **Current Ownership**: Name of organization that currently owns the product. This ownership attribute will be used to limit access of descriptor file information to downstream supply chain members. As a new company takes ownership of the drug this attribute will be re-assigned to the buyer. This feature will prevent other organizations from having inappropriate access to inventory level information of the buyer. Supply chain members will not be able to see who the current owner is unless proper privilege has been provided.
EPCs will be generated at the unit of use level. This means that a unique EPC will be generated at the bottle, blister pack, and strip pack level of packaging. The EPC tag will also be physically attached to this packaging.

The creation of the Manufacturer EPC makes it incumbent upon the manufacturer to maintain an Internet accessible database storing descriptor file information about each EPC. Queries for information about this product from downstream supply chain partners, as well as end users, will be redirected from the central clearing house database to the Manufacturer Database (MDb). This database must be properly secured and permission levels assigned to supply chain members to limit the levels of access. The manufacturer will also maintain a local database (LDb) containing intra-organizational information about their EPCs that is not publicly accessible (although is subject to FDA inspection). Depicted below are examples of records in the MDb, ADb, LDb.
Example of a Basic Manufacturer EPC Descriptor File in MDB

<table>
<thead>
<tr>
<th><strong>EPC:</strong> &lt;EPC NUMBER&gt;</th>
</tr>
</thead>
</table>

**Open Information: Track & Trace**

Manufacturer EPC Number: <96 bit unique code>
Global Status: <Active, Expired, Terminated, Recalled, Damaged, Returned, Sample>
Manufacturer EPC Creation Date: 12/31/2002
Formulation Manufacturer: MI
Formulation Creation Date: 01/01/2003
Formulation Expiry Date: 01/01/2013
Formulation Lot Number: 1401a
Intended Market: United States

**Authentication: <Authentic, Invalid>**

**Open Information: Product Description**

Marketed Name: Panacea (Country Specific)
Scientific Name: Someinexplicablylongthing
Active Ingredient List: x, y, z
Inactive Ingredient List: a, b, c
Product Catalog Link: www.website.com
Dosage Instructions: <Normal, Geriatric, and Pediatric>
Contra-Indications: abc
Overdose Instructions: xyz
Helpline: 555-1111

Compiled March 2003
Example of Basic Audit Database EPC Record

<table>
<thead>
<tr>
<th>EPC: &lt;EPC NUMBER&gt;</th>
</tr>
</thead>
</table>

**Secured Information: Highly Restricted Access – FDA**

Current Owner: R1  
Last Updated: 6/1/2003 14:42:08  
Last Sign-Off: Joe Supervisor

**Manufacturer Level Privilege: Upstream Tracking**

Ingredient Supplier Associated EPCs: 1,2  
<Track & Trace information for EPC 1>  
<Track & Trace information for EPC 2>  
Bulk Supplier Associated EPCs: 3  
<Track & Trace information for EPC 3>

**Manufacturer Level Privilege: Downstream Tracking**

Product Sold To: D1  
Product Sale Date: 2/1/2003

**Distributor Level Privilege: Upstream Tracking**

Product Purchased From: M1  
Product Purchase Date: 2/1/2003

**Distributor Level Privilege: Downstream Tracking**

Product Sold To: R1  
Product Sale Date: 3/1/2003

**Retailer Level Privilege: Upstream Tracking**

Product Purchased From: D1  
Product Purchase Date: 3/1/2003
### Retailer Level Privilege: Downstream Tracking

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Sale Date:</td>
<td>4/1/2003</td>
</tr>
<tr>
<td>Quantity Sold:</td>
<td>100</td>
</tr>
<tr>
<td>Product Sale Date:</td>
<td>5/1/2003</td>
</tr>
<tr>
<td>Quantity Sold:</td>
<td>200</td>
</tr>
<tr>
<td>Product Returned To:</td>
<td>Return Co.</td>
</tr>
<tr>
<td>Product Return Date:</td>
<td>6/1/2003</td>
</tr>
<tr>
<td>Quantity Returned:</td>
<td>700</td>
</tr>
<tr>
<td>Reason for Return:</td>
<td>Damaged in Transport</td>
</tr>
<tr>
<td>Information Related to Return Policy:</td>
<td>Other manufacturer specific information related to return policy</td>
</tr>
</tbody>
</table>

### Returns Handler Privilege: Upstream Tracking

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Received From:</td>
<td>R1</td>
</tr>
<tr>
<td>Product Receipt Date:</td>
<td>7/1/2003</td>
</tr>
<tr>
<td>Quantity Received:</td>
<td>700</td>
</tr>
<tr>
<td>Reason for Return:</td>
<td>Damaged in Transport</td>
</tr>
<tr>
<td>Information Related to Return Policy:</td>
<td>Manufacturer specific information related to return policy</td>
</tr>
</tbody>
</table>

### Returns Handler Privilege: Downstream Tracking

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Shipped To:</td>
<td>M1</td>
</tr>
<tr>
<td>Product Ship Date:</td>
<td>8/1/2003</td>
</tr>
<tr>
<td>Quantity Shipped:</td>
<td>700</td>
</tr>
</tbody>
</table>

### Transportation Provider T1

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Shipped From:</td>
<td>M1</td>
</tr>
<tr>
<td>Pickup Date:</td>
<td>4/1/2003</td>
</tr>
<tr>
<td>Product Shipped To:</td>
<td>D1</td>
</tr>
<tr>
<td>Delivery Date:</td>
<td>4/3/2003</td>
</tr>
</tbody>
</table>

### Medicine Authenticator A1

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Received From:</td>
<td>D1</td>
</tr>
<tr>
<td>Product Receipt Date:</td>
<td>6/5/2003</td>
</tr>
<tr>
<td>Quantity Validated:</td>
<td>1000</td>
</tr>
<tr>
<td>Quantity Rejected:</td>
<td>0</td>
</tr>
</tbody>
</table>
Example of Basic Local Database (LDb) Record for a Manufacturer

<table>
<thead>
<tr>
<th><strong>EPC:</strong> &lt;EPC NUMBER&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manufacturer Audit Db Copy: Upstream Tracking</strong></td>
</tr>
<tr>
<td>Ingredient Supplier Associated EPCs: 1,2</td>
</tr>
<tr>
<td>&lt;Track &amp; Trace information for EPC 1&gt;</td>
</tr>
<tr>
<td>&lt;Track &amp; Trace information for EPC 2&gt;</td>
</tr>
<tr>
<td>Bulk Supplier Associated EPCs: 3</td>
</tr>
<tr>
<td>&lt;Track &amp; Trace information for EPC 3&gt;</td>
</tr>
<tr>
<td><strong>Manufacturer Audit Db Copy: Downstream Tracking</strong></td>
</tr>
<tr>
<td>Product Sold To: D1</td>
</tr>
<tr>
<td>Product Sale Date: 2/1/2003</td>
</tr>
<tr>
<td><strong>Manufacturer Validation Information</strong></td>
</tr>
<tr>
<td>Last Owner: John Manager</td>
</tr>
<tr>
<td>Last QA: Jane Checker</td>
</tr>
<tr>
<td>Last QA Date: 2/1/2003</td>
</tr>
<tr>
<td><strong>Manufacturer Telemetric Information</strong></td>
</tr>
<tr>
<td>DateTime: 2/1/2003 12:00</td>
</tr>
<tr>
<td>Location: ReaderA01</td>
</tr>
<tr>
<td>DateTime: 2/1/2003 11:00</td>
</tr>
<tr>
<td>Location: Reader A02</td>
</tr>
</tbody>
</table>
**Distributor Component**

**Pass-Through Distributor**

These distributors buy drugs from the manufacturer and do not break bulk before shipping product to another distributor or retailer. The Pass-Through Distributor will use the Manufacturer EPC to track the drugs internally. They will add the following information to the Manufacturer EPC descriptor file:

- Set the Current Ownership attribute.
- Record date of receipt of the product and where bought from.
- Record date of sale of the product and name of buying organization.

In addition to this information that will exist in the Manufacturer EPC descriptor file stored at the manufacturer, the distributor will also track other information locally. This information includes telemetric data and stock related information.

**Break-Bulk Distributor**

These distributors resell drugs in smaller packages than the size in which the manufacturer sells them. For example, a manufacturer may sell their drug in 1000 tablet bottles, and a Break-Bulk Distributor may break these into 100 tablet bottles.

The Break-Bulk Distributor must generate a new EPC for the new unit-of-use level packaging. This new Distributor EPC will contain all the original properties of its parent Manufacturer EPC through inheritance. *These new EPCs will be created with attendant Descriptor Files that will now reside in a database maintained by the Break-*
**Bulk Distributor.** This Distributor Database (DDb) will need to meet all the requirements outlined for the Manufacturer Database outlined previously.

The Break-Bulk Distributor will now become the target location that downstream partners query in order to gain product specific information. The new and independent EPC creation is a necessary step for two reasons. First, the original Manufacturer EPC does not provide a granular means of locating a specific unit-of-level package once the original pack is broken into smaller packs. Ensuring unit-of-level trace ability is important to counterfeit prevention because in the absence of this mechanism, duplicate products would be associated to the same EPC.

The need for new EPCs at this more granular level is clear and absolute. The need for a new Distributor EPC is less absolute. This latter implementation provides for the privacy of break-bulk distributors who do not want the original manufacturer to have additional information about what quantity their product is ultimately sold in. If the distributor does not create their own EPC and maintain it themselves then this information must be provided to the manufacturer. Hence a Distributor EPC that inherits all the properties of the Manufacturer EPC allows for the passing of relevant information downstream from the manufacturer without passing distributor information upstream.

An alternative scenario that this distributor could pursue would be to create new EPCs and ask the manufacturer to attach these EPCs as part of the original Manufacturer EPC. These EPCs would then still carry the manufacturer’s identifying code and would
be issued by the manufacturer to the distributor upon request. Therefore when these EPCs were queried later in the supply chain, the queries would be redirected to the MDb. This would greatly reduce price of the Auto-ID infrastructure on the Break-Bulk Distributor, but at the cost of revealing additional information about their operations. The current schema supports the ability for individual distributors to make this business decision as they see fit.
**Retailer Component**

Retailers include pharmacies, hospitals, and alternate site providers. Retail organizations are the last organization to have ownership of the EPC before it is permanently killed.

Upon receipt of product at the retailer distribution center the retailer will add the following information to the Manufacturer or Distributor EPC descriptor file.

- Set the Current Ownership attribute
- Record date of receipt of the product and where bought from.
- Record date of receipt of the product to the store/hospital front.
- Record date of sale to end-user.
- Set Status of EPC to Terminated – which will physically de-activate the embedded tag. (Note: Tag will also de-activate when product expiry date is reached).

In addition to this information that will exist in the global EPC descriptor file, the retailer will also track other information locally. This information includes telemetric data and stock related information.
End User Component

The end user is the final customer; the end user will not resale the product. This includes the patient who takes the medication, as well as the doctor or nurse applying the appropriate consumption dosage.

Upon purchase of the medicine, the end user will receive a printout copy of the EPC code associated with his medication. In order to protect consumer privacy, the Auto-ID tag itself will be killed at the point of purchase. By giving the consumer the printout of the EPC tags though, either on the receipt or on the insurance claim documents, any future recalls can be facilitated. In addition, the consumer can look up their specific EPCs on the web to ensure that they have received an authentic product, as well as finding information about usage.

It is important to remember that the dispensing outlet that provides the medication to the end user may not be providing the full unit-of-use level packaged product to the individual. Therefore multiple doses may emanate from the same EPC and one individual may receive medication from multiple EPC tagged products. At point of sale, the descriptor file associated with each EPC will have the “Quantity” attributed deducted by the number/amount of medication taken from the unit-of-use level container and given to the end user. Once the Quantity attribute becomes zero the “Global Status” attribute will be set to “Terminated” and the embedded tag will be automatically physically deactivated.
Other Supply Chain Members

3rd Party Return Handlers

The members of the supply chain often handle the return of expired or damaged products for the pharmaceutical industry. Distributors and retailers will send returnable products to these providers. These providers in turn will determine the exact nature of the return agreement between the manufacturer and the buyer. This agreement can be different for each product, manufacturer, and buyer. Supply chain members turn to these providers as a result of the complexity involved in sorting through the return process.

In an RF-enabled supply chain, the return handlers will need to purchase this technology. They will need to validate that the EPCs they have received are valid and that fake products are not being introduced into the supply chain in the reverse direction. EPC tracking will also be valuable to these participants, because the descriptor file will now contain the rebate related information within it, reducing the cost of operations.

3rd Party Authentication Firms

These providers exist in order to provide some level of authenticity checking today. Manufacturers will hire authentication firms to test samples of their product throughout the supply chain. This sampling is optimized to look for areas of high counterfeiting. The border regions with Canada and Mexico are subjected to more frequent inspection, as are drugs on allocation or known to be in high demand.

Authentication firms will need to become RF enabled. The need for these organizations will not go away with RF technology, but their capabilities for detection
will be enhanced. RF technology cannot ensure that the pills themselves have not been tampered with, therefore visual inspection is still recommended. With better tracking though, authentication firms will be much better equipped to test specific areas or drugs for the possibility of counterfeits. The RF-enabled scenario, by providing better information, will allow authentication firms to conduct far more precise investigations while using the same sample size.

3rd Party Transportation Providers

Transporters of medicines will also need to adopt the RF infrastructure. This will ensure that medicines are tracked even during transport. In addition, it will become possible to record environmental conditions and inventory pipeline flow with RF enablement. A truly secure supply chain requires that these intermediary participants also become RF-capable.

Non-RF-Capable Intermediaries

During the initial years of implementation, there will be participants, who for financial reasons are unable to adopt RF technology as rapidly as larger players. These organizations will not be prevented from taking part in the supply chain, but will be ultimately required to become RF-enabled. Dealing with a hybrid supply chain during the interim period is discussed in a later section.

Governmental Organizations

The FDA, as the ultimate governing body, will be allowed access to the Audit Db when counterfeits are detected. Sensitive, but unrelated information, such a product pricing, revealed to the FDA must remain confidential within the FDA.
Counterfeit Detection within a Fully RF-Enabled Supply Chain

With the establishment of a Manufacturer EPC all unit-of-use level medicines can be tracked, without visual inspection, throughout the full, authorized supply chain. Every time an EPC tracked product is received by a supply chain member, the new member’s receipt confirmation will be compared against the descriptor file to make sure that there are no discrepancies. This automatic checking of the audit trail with each movement of the product will provide a continuously monitored environment to ensure that no product are ever moved outside of the authorized supply chain. This auditing mechanism will work somewhat differently when supply chain partners without RF-enabled hardware are involved. The Auto-ID solution in a hybrid environment is described in a later section.

As noted previously, the EPC is not the only way to detect counterfeit. Other measures are also required, including tamper proof containers, formulation level chemical tracking, and packaging changes. Some scenarios below outline how all of these anti-counterfeit technologies can combine to ensure the highest levels of product authenticity for products sold wholly within the authorized, RF-enabled, supply chain.
Table of Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
<th>AutoID Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fake EPC</td>
<td>Fake EPC label put on package.</td>
<td>EPC not found in DB.</td>
</tr>
<tr>
<td>Internet Rx</td>
<td>Web Pharmacy mails fake.</td>
<td>Consumer checks EPC against DB and determines fake.</td>
</tr>
<tr>
<td>Product Return</td>
<td>Product to be returned is resold as</td>
<td>Attempt foiled because EPC status marked as “Return”.</td>
</tr>
<tr>
<td></td>
<td>authentic.</td>
<td></td>
</tr>
<tr>
<td>Dumpster Diving</td>
<td>Discarded pack resold with fake.</td>
<td>Attempt foiled because EPC status marked as “Sold”.</td>
</tr>
<tr>
<td>Expired Product</td>
<td>Expired product resold.</td>
<td>Attempt foiled because EPC status marked as “Expired”.</td>
</tr>
<tr>
<td>Sample Product</td>
<td>Product sample resold as authentic.</td>
<td>Attempt foiled because EPC status marked as “Sample”.</td>
</tr>
<tr>
<td>Diverted Product</td>
<td>Product sold in foreign market</td>
<td>Attempt foiled because EPC shows intended market.</td>
</tr>
<tr>
<td></td>
<td>diverted to the U.S.</td>
<td></td>
</tr>
<tr>
<td>Package Tampering</td>
<td>Product seal broken and medicines</td>
<td>Attempt foiled because EPC also ripped, triggering alarm.</td>
</tr>
<tr>
<td></td>
<td>replaced.</td>
<td></td>
</tr>
<tr>
<td>Formula Tampering</td>
<td>Poor quality medicine shipped in</td>
<td>Attempt foiled through formula testing policy triggered based on who authentic product.</td>
</tr>
<tr>
<td></td>
<td>authentic product.</td>
<td></td>
</tr>
</tbody>
</table>

Scenario 1: Introduction of fake EPC by Distributor Diluting Product

Step 1: Manufacturer, M1, sells product to distributor, D1.

- Descriptor file record under owner M1 records sale to D1
- Descriptor file record under owner D1 records purchase from M1
- Change of ownership attribute triggers descriptor file record audit to verify that M1’s “Sold To” information is the same as D1’s “Purchased From” information.
- Authentication flag set to “Authentic”.

Step 2: D1 sells product to distributor, D2.

- Descriptor file record under owner D1 records sale to D2
- Descriptor file record under owner D2 records purchase from D1
• Change of ownership attribute triggers descriptor file record audit to verify that D1’s “Sold To” information is the same as D2’s “Purchased From” information.

• Authentication flag set to “Authentic”.

Step 3: D2 dilutes purchased contents and applies new fake EPC to newly created boxes and sells everything to retailer, R1.

• At point of sale, R1 attempt to record purchase of fake EPC throws error because EPC validation not possible from manufacturer.

• Authentication flag set to “Unable to Validate”.

• R1 follows up with D2 and M1 to locate that problem happened at D2 site.

  Appropriate action taken.

Scenario 2: Counterfeit Product Shipped by Internet Pharmacy

Step 1: Consumer buys medicine from Internet Pharmacy that sells 1 authentic and 1 counterfeit product to the consumer.

• Due to privacy restrictions, Auto-ID tag is killed at point of sale by Internet Pharmacy.

• Consumer is provided a Manufacturer EPC number for both products purchased at time of purchase.

Step 2: Consumer checks legitimate Manufacturer EPC tag against Auto-ID website.

• Consumer enters first (legitimate) EPC into website.

• Auto-ID website reads EPC number and re-directs query to public web site for manufacturer of the legitimate EPC.
• Consumer sees public information about medicine and that the authentication attribute is set to “Authentic”

Step 3: Consumer checks un-authentic Manufacturer EPC tag against Auto-ID website.

• Consumer enters EPC number at website.

• If EPC doesn’t exist, Auto-ID website warns user that product should not be used and ask for additional information to resolve the problem.

• If EPC contains a known manufacturer’s address, then user is redirected to manufacturer’s public website.

• At manufacturer’s website, depending on whether EPC is non-existent, duplicate, or inappropriate, consumer is informed of problem and what needs to be done.

**Scenario 3: Using Returned Products For Counterfeit**

Step 1: R1 ships damaged products to 3rd party Return Handler.

• R1 marks “Status” attribute for associated EPCs as “Damaged”. R1 enters information on where product has been shipped to and when.

Step 2: R1 employee takes damaged product and resells it to another distributor, D3. Or employee at return handling company resells product to another distributor, D3.

Step 3: D3 sees associated EPCs as marked “Damaged” in the descriptor file and refuses sale.

**Scenario 4: Dumpster Diving – Retrieving Empty Containers for Counterfeit**

Step 1: Hospital, H1, discards old boxes in dumpster. Vandal recovers boxes and sells to counterfeit manufacturer, CM1.
Step 2: CM1 unable to use container because EPC tag was killed at point of sale to H1.
  
  • EPC tag is physically broken so tag cannot be turned on by software.
  
  • EPC number has been retired so it cannot be reused even if tag is operational.

Scenario 5: Selling Expired Product as Authentic

Step 1: R1 realizes shelf life has been reached on product but tries to sell it to distributor, D2.

Step 2: Upon receipt D2 reads EPCs as expired and rejects shipment.

Scenario 6: Selling Sample Product as Authentic

Step 1: Distributor D2 has extra product to be sold as sample only. Employee takes this product and sells it to retailer R1.

Step 2: Upon receipt R2 reads EPC status as marked “Sample” and rejects shipment.

Scenario 7: Diversion – Selling Products from an Authorized Channel to an Unauthorized Channel.

Step 1: Distributor D2 buys product sold by manufacturer, M1, in the Canadian market.

Step 2: D2 moves product across border and attempts to sell to retailer, R1, in U.S. market.

Step 3: Upon receipt, R1 detects that “Intended Market” attribute on EPC descriptor file indicates “Canada”. Shipment is rejected and appropriate action taken against distributor

Step 3b: Alternatively, M1 is alerted that R1 has received EPCs marked for the Canadian market.

  • M1 is not provided any information besides this due to privacy restrictions.
• “Intended Market” is considered an open attribute and only on violation of this restriction is a report made to the manufacturer on the downstream location of this item.

• M1 takes appropriate action to rectify problem.

Examples of Counterfeit Detection using Alternative Technologies and AutoID

Scenario 8: Package Tampering

Step 1: D2 opens received product bottles and removes legitimate contents. This breaks difficult to replicate seal.

• D2 rebottles good medicine in a new container with no EPC.

• D2 fills original bottle that has EPC, with counterfeit product, but no seal.

Step 2: D2 sells container with no EPC to region that doesn’t use EPC infrastructure.

Step 3: D2 sells container with EPC, but fake product, to R1.

Step 4: R1 receives product into distribution center.

• R1 knows from EPC trail that product was purchased from infrequent supplier.

• Therefore R1 enforces Visual Inspection policy on products with these EPCs. This requirement is automatically added onto the local copy of the EPC record at point of purchase by a business rules engine specific to the retailer.

Step 5: Visual Inspection at R1 discovers lack of seal

• Product is taken out of DC.

• Appropriate action is taken against distributor.
Scenario 9: Formulation Tampering

Step 1: D2 opens received product bottles and removes legitimate contents. This breaks seal.

- D2 rebottles good medicine in a new container with no EPC.
- D2 fills original bottle that has EPC, with counterfeit product.
- D2 uses in-house sealing technology to reseal original bottle so tampering is not readily apparent.

Step 2: D2 sells container with no EPC to region that doesn't use EPC infrastructure.

Step 3: D2 sells container with EPC, but fake product, to R1.

Step 4: R1 places product on shelf.

- R1 knows from EPC trail that product was purchased from infrequent supplier.
- Therefore R1 enforces Point-of-Sale Drug Testing policy on product dispensed from this EPC. This requirement is automatically added onto the local copy of the EPC record at the pharmacy by a business rules engine specific to the retailer.
- At point of sale, the pharmacist sees this testing requirement flash up on his computer screen because the EPC has been removed from the shelf.

Step 5: Pharmacist conducts drug authenticity test with testing kit and find products to be counterfeit.

- Consumer is given alternative product.
- Retailer takes appropriate actions against distributor.
Supply Chain Coordination with Members Without RF Infrastructure

Using an RF-enabled supply chain will greatly reduce the problem of counterfeits but it is expected to take many years before the domestic pharmaceutical industry can become fully RF enabled. Initially, it is expected that major manufacturers, the big three distributors (Cardinal, McKesson, and AmerisourceBergen), and large retailers will quickly implement RF infrastructure. In this initial scenario, there will still be significant transportation of products outside of these players. The RF scenario proposed must be robust enough to support a hybrid supply chain architecture comprised of RF-enabled players and legacy partners (those without RF technology).

When medicines leave the RF-enabled supply chain there will be an unresolved gap in the distribution chain. In practical terms this means that when an RF-enabled company sells their product to a legacy partner, the “Sold To” field in the Audit DB can not be verified. This is because the buying company will not transmit receipt of the product to the Audit DB. Similarly, when a legacy partner sells their products to an RF-enabled partner, the “Purchased From” field cannot be validated against the Audit DB. While this is not the preferred scenario, it does not defeat counterfeit protection. When the product is re-introduced into the supply chain, the product EPCs will still be validated against the Manufacturer DB to prove that these products are authentic. Of course, it is possible that legacy partners could take these products and switch the contents inside with fakes and then resell the adulterated product into the RF supply chain. BUT, this is also possible with RF-enabled players, as outlined in Scenario 8 and 9. The countermeasure against package or formulation tampering must rely on incorporating
hardware technologies like tamper-proof packaging and chemical formulary additives in conjunction with RF technology. This remains true whether the product is been shipped inside or outside the RF-enabled supply chain.

There are a few process changes that must be implemented though to handle the hybrid supply chain scenario. The product verification method works on the ability to match the seller’s “Sold To” field to the buyer’s “Purchased From” field. As mentioned earlier, this will not be possible when a legacy partner is part of the transaction. In order to prevent an alert from being generated, the RF-enabled partner will set the “RF Enabled Partner” field to “No” in the appropriate EPC descriptor files. When this flag is set, the normal auditing procedure will be skipped. Authenticity will be verified by checking the EPC when the product is re-introduced into the supply chain.

Moving product through a hybrid supply chain will also mean that the Audit Db will be incomplete. This database can be used to understand exactly where counterfeiting is occurring. But in the case of selling to legacy partners this capability is lost because the product could be exchanged between multiple legacy partners before coming back into the RF enabled supply chain. Therefore, when a counterfeit is found, it will be more difficult to understand which organization actually did the counterfeiting. This is unfortunate but unpreventable. The burden of requiring equivalent paperwork detailing transactions outside the RF supply chain, at the unit of use level, is too costly and onerous on smaller organizations. In this scenario, law enforcement will have to attempt to reconstruct events to determine the source of the counterfeiting. But while tracking the
guilty party becomes harder, the ability to prevent the introduction of the medicine into
the supply chain remains unassailable. As explained earlier, fake EPCs will still be
detected upon re-introduction to the supply chain. It is imperative though, that retailers
selling prescription drugs be RF-enabled in order to validate the EPC at the final point of
sale. The cost of this capability should not be prohibitive to the retailer as need not buy
any EPC tags or keep a local database to implement this basic requirement. A small
retailer would only need a single reader to scan the EPC of each product before
dispensation. It is expected that even the smallest of retailers will be able to afford the
one-time, one hundred dollar cost of this reader.
VI. Conclusion

Counterfeit medicines pose a significant and increasing threat in the United States. The global threat has long been recognized, but lack of governmental and technology infrastructure in developing countries makes implementing a global solution challenging. There is no reason though that countries and industries capable of implementing a solution today should not pursue these ends as fast as possible. Financial concerns for adopting the solution presented in this document must be weighed against the reality that human lives are at risk. In deference to the legitimate concerns of the industry, this proposal has attempted to design a multi-staged approach to securing the supply chain. The suggested multi-year time frame for large industry players to introduce RF capability to track the subset of most frequently counterfeited medicines should provide plenty of time for compliance. RF technology alone though, will not secure the supply chain. As outlined in this proposal, additional legal enforcement, greater awareness of the problem by the industry and consumers, and better implementation of existing technical countermeasures are all needed in addition to RF-enablement. With the incorporation of this full set of techniques, the seemingly intractable problem of counterfeit medicines can be greatly mitigated. It is important to keep in mind, that more than anything else, it is the willingness of industry and governmental participants to work together that will determine our capability to secure the domestic pharmaceutical supply chain.
References


<http://www.who.int/medicines/organization/qsm/activities/qualityassurance/counterfeit/faq_counterfeit.doc>

<http://www.who.int/medicines/organization/qsm/activities/qualityassurance/counterfeit/counterfeit_info_facts.shtml>