Rx-360 Supply Chain Security White Paper:

Threats and Monitoring Processes

18 May 2012

This White Paper was developed and authored by the members of the Rx-360 Supply Chain Security Market Monitoring Working Group:

Lew Kontnik, Amgen
Bill Eubanks, Takeda
Charlotte Hicks, Doe & Ingalls
Jeremy Baumann, Takeda
Jyrki Syvaeri, Boehringer Ingelheim
Michael Broughton, Eli Lilly
Matt Yedwabnick, Amgen
Kola Stucker, Bristol-Myers Squibb
Karine Roth, Novartis
Kevin Weaver, Johnson & Johnson
Leslie Glassman, Abbott
Matt Whitt, GSK
Anthony Zook, Merck & Co

Contents

Introduction and Overview 5
Counterfeit, Unapproved, and Diverted Drugs (CUDD) Definition and Sources 5
Counterfeit Products 6
Unapproved Products 7
Diverted Products 8
CUDD Distribution 9
Avastin Counterfeit Example 9
Internet-based Distribution 10
Other Sources of Distribution 11
SCS Monitoring Practices 11
Product Security Threat Risk Assessment 12
Threat and Signal Database and Intelligence System 13
Theft Monitoring and Analysis 13
Monitoring the Internet 14
Monitoring of Physical Operations 15
Leveraging Existing Internal Systems and Processes 16
Complaints 16
Adverse Events 16
Returns 16
Wholesaler Audits 16
Quality Audits 17
Call Center 17
Authorized Distributor of Record 17
Product and Material Destruction 17
Product Analysis 18
Product Sales Analysis 18
Product Security Features and Serialization 18
Communication and Education 19
Internal Communication and Education 19
External Communication and Education 19
Working with Outside Agencies 20
Test Purchase Capabilities 20
Incident Management 21
Reporting of Incidents 21

What Needs to be Communicated and How to Communicate 22
Conclusion 22
Appendix A – Checklist of Monitoring Programs/Techniques 23

Introduction and Overview

The distribution and sales of Counterfeit, Unapproved and Diverted Drugs (CUDD) are a global concern for pharmaceutical patients, health care professionals, regulators and manufacturers. Counterfeit drugs are not equivalent to the genuine product in safety, efficacy and quality. At best, they are of unknown composition and may be ineffective, and at worst harmful to patients. Unapproved medicines are drug products that have not been approved by a country's health authority for product quality and efficacy or patient safety. Diverted drug products may be genuine but may not have the properties that doctors/pharmacists expect (if they are imported products) and may be subject to mishandling and inappropriate storage conditions that may impact product quality. They typically contain packaging and information leaflets in foreign languages for foreign markets that are not approved by the local health authority, and are considered misbranded. Considering that patient safety is the priority for industry, pharmaceutical manufacturers should have a process dedicated to the identification and prevention of CUDDs in the marketplace.

This document provides a general overview of the definitions, sources, and distribution of CUDDs in the finished form, as well as a high level summary of Supply Chain Security (SCS) monitoring practices and tools that pharmaceutical companies can use to help detect, deter, and to establish appropriate control for CUDDs in the supply chain. It also refers to the concept of a Management System Maturity Model: a concept being introduced by the Rx-360 Supply Chain Security (SCS) initiative. A Maturity Model will be used in subsequent versions of this document to drive the measurable and sustainable improvement of SCS toward a comprehensive Management System. This document is meant to provide a basic understanding but does not seek to provide detailed guidance.

Counterfeit, Unapproved, and Diverted Drugs (CUDD) Definition and Sources

There are a variety of factors that make medicines appealing to those individuals involved in the making, selling and/or distribution of CUDD.

- Patients and medical staff have a non-discretionary need for medicines
- Medicines are often high value relative to their size and weight, and therefore profitable, easily smuggled, and shipped
- The authenticity of medicines and packaging is difficult to verify by customers and patients
- There can be significant price differences between countries and even distribution chains within countries
- Demand can exceed supply due to product shortages, disease out-breaks, or natural disasters.
- Prosecution of CUDDs is often a low priority for law enforcement with a low penalty if convicted which further impacts the patient community

This section serves as a primer for companies looking to understand the definition of Counterfeit, Unapproved and Diverted Drugs (CUDD) products, as well as the sources from which they originate.

While the vast majority of CUDD incidents to date have apparently been motivated by profit/greed, it is important for readers to keep in mind that in today's world, terrorists may also be motivated to use counterfeit medicines as a tool.

Counterfeit Products

Definition

Because laws vary between countries, so do definitions concerning counterfeit products. In general, counterfeit products are made or altered by a party other than the manufacturer with intent to deceive. Because each country defines counterfeit differently, the World Health Organization's (WHO) definition will be used in this paper.

WHO Definition: *A counterfeit medicine is one which is deliberately and fraudulently mislabeled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products. 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.*[1,2,3,4]

As used herein, this definition is based on the "deliberate and fraudulent" aspect of the crime and is not predicated primarily on any patent or other intellectual property infringement. It is also important to distinguish between substandard products and counterfeit products. Substandard products are medicines of poor quality that were manufactured with the noncriminal intentions and appropriate practices.

Sources

Generally, the maker of the counterfeit knows that the product being made is not genuine. At times the manufacturer will conspire with the first level of distribution to make a product that meant to deceive later recipients into believing the product is genuine. Once it is in the market place, the counterfeiter has achieved his purpose—sales for a profit.

---

[1] http://www.who.int/medicines/services/counterfeit/overview/en/

[2] http://www.fda.gov/Drugs/DrugSafety/ucm169898.htm **USFDA Definition:** U.S. law defines counterfeit drugs as those sold under a product name without proper authorization. Counterfeiting can apply to both brand name and generic products, where the identity of the source is mislabeled in a way that suggests that it is the authentic approved product. Counterfeit products may include products without the active ingredient, with an insufficient or excessive quantity of the active ingredient, with the wrong active ingredient, or with fake packaging.

[3] **Definition, EU**: According to the Falsified Medicines Directive, the definition of counterfeited products is any medicinal product with a false representation of Identity, Source and/or History.
Identity, including packaging, labeling, name or composition in regards to ingredients, including excipients, and the strength of those ingredients.
Source, including manufacturer, country of manufacturing, country of origin or marketing authorization holder.
History, including the records and documents relating to the distribution channels used.
This definition does not include unintentional quality defects and is without prejudice to infringements of intellectual property rights.

[4] Pharmaceutical Security Institute: For Counterfeit Incident Submission (CIS), *A* counterfeit incident is the discovery of a medicine which was deliberately and fraudulently produced and/or mislabeled with respect to identity and/or source to make it appear to be a genuine product and applies to both branded and generic products. Counterfeit products may contain less than or more than the actual amount of active ingredient in the authentic version. The product may even be authentic, but be repackaged in counterfeited packaging. Any incident submission involving these types of products, including those where only counterfeit packaging has been found, is identified in Counterfeit Incident Submission (CIS) as a counterfeit incident.

Counterfeit products present themselves in one of two of ways: partially or entirely counterfeit. Entirely counterfeit products are composed of both counterfeit drug and packaging while partially counterfeit products will have either authentic product or packaging. Below is a list of some sources for counterfeit and authentic product and packaging:

Authentic packaging:

- Waste stream from the original manufacturer
- Original Equipment Manufacturer (OEM) supplier of original packaging
- Waste stream at hospitals and clinics
- Returned expired product.

Authentic product:

- Repackaging of bulk material
- Diverted materials (see diverted product below)

Counterfeit packaging:

- Professionally printed material
- In-house amateur designed material

Counterfeit product:

- Non-registered drug manufacturers
- Small cottage producers

In addition, tampered products should also be considered counterfeit. Tampered products are the intentional or improper unauthorized altering of a genuine drug product without the knowledge of the product's owner or eventual user. Tampering typically involves manipulation of the genuine drug product such as replacing the genuine label with a counterfeited label or substitution of the genuine product with some other drug product or product substitute.

Unapproved Products

Unapproved products are products that are not authorized for sale by the drug regulatory authority in the country where they are being sold. They may (or may not) be approved in other countries. These products could be unapproved, or products that make claims of therapeutic benefit without regulatory acknowledgement. They are often imported illegally.

Definition

A product must be approved (i.e., have marketing authorization) by the country drug regulatory agency before that product can be legally sold within that country. Products approved in one country cannot be sold and/or transferred into another without gaining authorization from the local regulatory agency.

Types of unapproved material

- Product that is not approved by the country's regulatory agency in which it is being sold/transferred
- Products made with Unapproved Active Pharmaceutical Ingredient (API) that is not registered with the local regulatory agency in the country in which you expect to sell the finished product.

Sources

Unapproved products are frequently imported or smuggled from developing countries; however, they can be produced domestically, sometimes by compounding pharmacists or local unauthorized manufacturers.

Diverted Products

Diversion can be viewed as unlawful, out of channel sales. The unlawful aspect can be legislative (e.g., prohibition of the importation of unapproved medicines), or contractual (e.g., violation of "own use" agreements prohibiting nursing homes or government agencies from reselling discounted product).

Definition

Diverted product is material that is redirected from the manufacturer's intended area of sale or destination to a different geography or distribution channel and includes a product that is inappropriately redirected from its intended course or end-user destination[5]*. Diversion is also known as gray market activity. The key criterion is that the product is genuine although it is possible that some counterfeits may be present in the mix. Note: Parallel trade*[6]*, the sale of product from one EU country in another, taking advantage of pricing differences is similar in pattern but is legal and explicitly protected within the EU.*

Sources

Below, are sources of international and domestic diverted product.

International Trade Arbitrage

Usually, it is not permissible to import medicinal products into a country without having the specific medicine approved for use and importation by the local drug regulatory authority. In some cases, the drug may be legal, but is smuggled into the second market through false declarations as to its nature and identity. All products traded without such permission are illegal, although they come from the original manufacturer. Again price differentials drive the source for diverted products.

In-Country Discounted Arbitrage

Diversion may occur within the same geographic area, within the same country or city. For example, incidents in Latin America include diversion cases in which government purchases of discounted drugs are diverted from state hospitals to the local street pharmaceutical markets.

---

[5] ***PSI Definition:*** Incidents of illegal diversion or for simplicity, diversion, of pharmaceuticals are included in CIS. Diversion occurs when a legitimate pharmaceutical product is approved and intended for sale in one market, but is then illegally intercepted and sold in another market. Many times, drug regulators in the second market have not formally approved the use of the diverted drugs. In some cases, the drug may be legal, but is smuggled into the second market through false declarations as to its nature and identity. Diversion may also occur within the same geographic area, within the same country or city. This type involves diverting discounted medicines from the intended group of consumers to an open market. For example, incidents in Latin America include diversion cases by which government purchases of discounted drugs have been diverted from state hospitals to the local street pharmaceutical market. All types of diversion incidents are tracked in CIS because of the inherently criminal nature of these operations and the potential to expose innocent patients to potentially harmful drugs due to the questionable handling and storage of these products while outside the normal distribution chain.

[6] Parallel importation is legal in some areas of the world.

While there are several sources of domestic arbitrage, key sources include repackaging of bulk products, rebated materials, theft/redistribution, charitable donations and reverse logistics.

- Repackaging bulk received by hospitals/clinics (may or may not be legal depending on country)
- Product purchased with contracted discounts may be diverted in violation of law or contract by the customer receiving the discount. Examples include the diversion into commercial channels of medicines sold at a discount for use in government sponsored or operated programs (e.g., 340B program in the US)
- Product returned for destruction can be diverted back into the distribution chain
- Theft and re-distribution of product during transport (cold chain product is especially vulnerable to quality deterioration due to inappropriate storage conditions)
- Charitable donations diverted back into legitimate trade supply (often in counterfeit packaging)
- Diverted product resulting from Fraud against the Government.

All types of counterfeiting and diversion incidents are tracked in Pharmaceutical Security Institute's Counterfeit Incident System CIS because of the inherently criminal nature of these operations and the potential to expose patients to potentially harmful drugs due to the questionable handling and storage of these products while outside the normal distribution chain.[7]

CUDD Distribution

Counterfeit, Unapproved and Diverted Drugs (CUDD) are often distributed through unauthorized channels or illicit markets. They can also be inserted into legitimate distribution channels. Many CUDD products are distributed through: on-line sellers such as trade boards, individual ads listings, on-line pharmacies; and illegitimate physical supply chain outlets such as flea markets/body builder networks and health/nutraceutical stores. They can also be sold through legitimate sources where the buyer is unaware they are buying a CUDD products. Different CUDD product types may be mixed. For example, counterfeit products may be mixed with genuine diverted product. Below is a summary of some of these distribution channels.

Avastin Counterfeit Example

In February 2012, the US FDA served notice that at least 19 US oncologists had purchase counterfeit Avastin through a complex distribution chain originating in Egypt and including Switzerland, Denmark, the UK and, finally the US. This case illustrates a number of the CUDD threats. First, the product being sold to US doctors was not fake US product, it was fake Turkish product. In other words, the counterfeits were inserted into a gray market supply chain that was already distributing unauthorized and diverted product. Several of the companies involved in this incident had already come to the attention of their local and international regulatory authorities and some had lost their wholesaling licenses. The owner of the company actually selling to the US doctors operated thousands of Internet pharmacies offering unapproved diverted products and the doctors involved could tell at a glance that the Avastin they received was not approved US product because the labeling was in French and Arabic. For more details on this case, please see Rx-360 article "Fake Avastin® Pulls the Curtain Back on Internet Pharmacies."[8]

[7] See: http://www.psi-inc.org/counterfeitSituation.cfm .
[8] See: http://www.rx-360.org/LinkClick.aspx?fileticket=agsCsw5i9B8%3d&tabid=274

Internet-based Distribution

Patients and self-medicating purchasers are increasingly using the Internet to obtain medicines and are at great risk of obtaining CUDD products. Some of the reasons for this trend include: lack of health care coverage, failure to appreciate the risk associated with online purchases, reluctance to see a doctor, attempting to obtain scheduled drugs due to addiction, and/or securing product without a prescription. Even more troubling is that some doctors and other medical professionals are also purchasing, and advising patients to purchase, from risky Internet sites. Unfortunately, the actual origin, safety and efficacy of these drugs are rarely known to the buyer. There are three primary paths that the Internet facilitates selling CUDD products: A business to customer relationship (B2C), business to business relationship (B2B) and customer to customer relationship (C2C).

B2C Internet Pharmacies

Recognizing the lack of regulation of on-line pharmacies, CUDD vendor/traders are increasingly using websites catering to patients (and sometimes medical practices) to sell CUDD product. Ease of creation of websites and, perhaps, demand by patients has caused the rapid proliferation of Internet Pharmacies. Many of operators of these enterprises create multiple connected sites, sometimes aimed at specific patient populations. Some also invite site visitors to become “affiliates”—i.e., encourage strangers to create their own sites and link to the “hub” site for payment processing and fulfillment. This is a common technique for expanding the reach of dangerous Internet Pharmacies.

B2B Trade Boards

Trade Boards (such as Alibaba and EC21) are another CUDD distribution channel. These sites cater to visitors who are seeking commercial/wholesale quantities of products. Individual offers are posted on “store fronts” created by sellers on the host Trade Board site. Some of the more well recognized Trade Boards (e.g., Alibaba) have internal policies that forbid the sale of prescription medicines—contacting these sites can be an effective means for removing prescription offers. These exchanges are of special concern because the sellers are seeking individuals/organizations interested in buying in commercial quantities intended for resale and/or further distribution.

C2C Exchanges

EBay and Craig’s List are examples of another type of exchange, based more on a consumer to consumer model. In some cases, patients no longer require medicines prescribed and look to sell them to another consumer. Again, EBay and some other exchange sites have internal policies forbidding the sale of prescription medicines. Exchange internal policing can be spotty, so it behooves manufactures to scan these sites. In some instances, criminal enterprises make use of these “individual” offers to sell limited quantities of medicines as a front for making connections for the sale of commercial quantities of product.

B2B Fax Blast/Direct Email

A long standing practice among secondary suppliers has been the use of faxes to doctors and pharmacists offering discounted or close out products. Direct mail is also used as a communication technique. Increasingly these offers contain diverted or unapproved products. At times, the product delivered is counterfeit as in the case of Avastin recently in the US and the UK.

Other Sources of Distribution

While the Internet makes up a large part of the CUDD distribution, physical distribution outlets also represent channels for distribution. These physical outlets can be divided generally into authorized and unauthorized channels.

Insertion of CUDD Products into the Authorized Supply Chain

There are numerous examples of authorized channels (pharmacies, clinics, medical practices, etc.) having dispensed or sold CUDD products. Cases include the recent introduction of counterfeit Avastin into US oncology practices and the distribution of fake Articinate to malaria patients in the Mekong.[9]

Authorized channels may acquire CUDD products due their own willful or negligent disregard of purchasing from authorized sellers, as appears to be the case in the Avastin situation. It can also result from the use of devious schemes in the secondary supply chain to hide to source of the products being offered, resulting in the unwitting purchase and dispensing of CUDD products.

Specialty Unauthorized Distribution Channels

There are a number of different types of specialty unauthorized distribution channels that create an opening for CUDD products to reach patients. Examples include some body builder suppliers that may promote off label use of some products, and some ethnic community shops that may sell medicines without authorization. Flea markets are another example where the vendors are likely to be faced with offers to buy CUDD product that they may in turn sell to patients/customers.

B2B Unauthorized *Detailing Operation*

Certain CUDD sellers have become aggressive to the point of hiring their own field sales reps to call on doctor's offices in the US to offer illegally imported, unapproved medicines to medical practices. Some of these field reps have adopted the practice of telling doctors that buying unapproved foreign medicines is legal, as long as it is purchased from a US company (not a correct statement of the law).

SCS Monitoring Practices

This section summarizes different monitoring practices that can help manufacturers identify, investigate and react to the sale and distribution of CUDD products. NOTE: the scope of this publication is restricted to "monitoring," another Rx-360 SCS publication will summarize Control and Enforcement techniques.

The sections below outline the use of:

- Product Threat Risk Assessment,
- Threat and Signal Intelligence System
- Theft Monitoring and Analysis
- Internet Monitoring
- Monitoring Physical Operations
- Using Existing Internal Systems
- Product Security Features
- Communication and Education

[9] Newton PN, et. al. Fake artesunate in Southeast Asia. *Lancet* 2001; 357: 1948-50.

- Working with Outside Agencies
- Undercover Purchases
- Incident Management

All of these categories of monitoring can produce important signals and analysis that help to identify CUDD problems and give companies an opportunity to respond and correct the problem. In launching a basic program, companies should build on their existing quality, product manufacturing and distribution processes. It is critical to establish a Threat and Signal Intelligence Process for acquiring and analyzing information and an Incident Management Process for confronting and responding to CUDD emergencies as they are identified.

A mature system would ideally have capabilities for executing all of the identified components and an optimized system would operate through a suite of processes that are directed and adjusted based on an ongoing explicit risk analysis and management process.

Product Security Threat Risk Assessment

Companies should have a process to help understand the CUDD threats they face based on the nature of the medicine, country/regional criminal environment and distribution model involved. The process should include identified tools and techniques for gathering information on the counterfeiting and diversion threats posed to different products in different markets and modeling particular threat levels.

Inputs to this process can be drawn from multiple sources. As a starting point for a company, there are industry organizations, like Rx-360, the Pharmaceutical Security Institute (PSI) and the Partnership for Safe Medicines,[10] that collect and communicate both threats and signals to the industry. The FDA and other national health authority websites also have information that should be considered as potential data points such as drug shortages, market withdrawals and recalls, counterfeit product reports, etc. Looking more broadly to other industries and sources (e.g., US Trade Representative Special 301 Report, International Customs seizure data) may increase the ability to see associations and patterns from a broader range of threat/signal data.

This analysis can be used in setting priorities for investment, action or identifying vulnerabilities. In addition to identifying a responsible team, a company will need to define criteria to analyze the threat level for its particular products and the information streams to assess geographic threat levels.

A basic approach to developing a Product Security Threat Risk Matrix is to review the relative likelihood or "desirability" of the criminal creation and distribution of CUDD. Possible parameters to consider could include:

- Risk of therapeutic class
- Pricing (e.g., high value)
- History of past CUDD for Product/Therapeutic Class
- Supply chain handling/transportation
- Price differentials (International pricing, discount structures)
- Pricing Reimbursement Structure
- Form of product (solid vs. injectable)

After having reviewed the overall vulnerability of the products to attack, it can be useful to analyze the country/market specific residual risks. In less developed countries, low value or mature products may be

[10] See: http://www.rx-360.org/, http://www.psi-inc.org/index.cfm, and http://www.safemedicines.org/

targets for counterfeiting and in certain countries there may be a much more active counterfeit or diversion problem. These problems may vary depending on the nature of the therapeutic class of the product. Likewise, the company may employ different sale and distribution practices for specific products or geographic markets (e.g., direct distribution of cold chain product to clinics may provide a more secure supply chain route than the use of distributor-wholesale network-retail sales). These differences can be reflected in the market specific risk analysis to help focus on the highest risk products and countries. Appendix A contains a high level example of a tool used by some companies.

Threat and Signal Database and Intelligence System

Companies should have a process and tools to gather, store, analyze and report on potential threats and signals indicative of counterfeit, diverted or unapproved products. This is a relatively new function for the industry and most likely will require dedicating resources, both financial and human, to establish.

At a minimum, there needs to be a record of the signals so that they can be reviewed and assessed. The record can range from a document or spreadsheet to a sophisticated relational database that can record the threat/signal data to use in the human or automated analysis and discovery of trends/patterns that may warrant further investigation by the company. The sooner a trend/pattern or a single data point is recognized as suspect or potential counterfeit, diverted or unapproved product and reported out to the appropriate company management/functions the more value this external monitoring has for the company.

The database should be suited to receive and organize information from the various monitoring systems described in this document. These inputs/signals should then be subjected to a process of analysis that identifies if there is a problem or CUDD incident that requires escalation and "crisis" management as discussed below.

Leading Practices—Emerging Opportunities

Sophisticated intelligence management or neural network systems that collect and automate the analysis of data to predict and provenance the counterfeit activity by region or by counterfeiter is considered a best practice. One classic example was the 1998 public health problem in Southeast Asia of counterfeit Artesunate.[11] By gathering chemical, mineralogical, biological and packaging data attributes, the evidence suggested a high probability that some of the counterfeits were manufactured in a particular Southeast region of China. By sharing this information with the appropriate law enforcement authorities, the criminals were located and arrested.

Companies wanting to explore this best practice may choose to start with reputable neural network freeware or a low cost software package that can be setup to conduct a feasibility study.

Theft Monitoring and Analysis

Companies should consider the periodic and routine review of both regional and global sources of cargo theft activity. While there are several sources, FreightWatch International runs one of the most robust systems for global activity and they supply annual and quarterly reports on both global and regional situational intelligence. Other sources of data include the Transportated Asset Protection Association (TAPA) Incident Information System reports available to its membership. The TAPA system reports on past events, and can thus be used as a tool in analyzing trends in the cargo theft world. In North America,

[11] Newton, PN, et. al. "A Collaborative Epidemiological Investigation into the Criminal Fake Artesunate trade in South East Asia", *PloS Medicine*, February 2008, vol. 5, Issue 2.

SC Integrity and CargoNet are two sources of information and they both provide similar date; but it is predominately focused on North American operations. An additional North American resource is the PSCSC – Pharmaceutical Supply Chain Security Council for real time reporting of cargo theft in North America. In Europe, EuroWatch is another organization that monitors cargo theft activity, and can be used to gather information throughout Europe and Western Russia.

Monitoring the Internet

There is a vast amount of information about a company's products (genuine and non-genuine) and their markets (legitimate and illicit) on the Internet. Through an Internet Monitoring program, companies should proactively monitor external marketplaces and websites to discover and identify rogue/illegitimate markets and sellers.

At the most rudimentary level, companies can use Google and other search engines to look for websites offering their products. This is likely to generate an overwhelming set of possible responses and it will become clear quickly that automated, organized systems are useful to categorize information by product, price, purported location, prescription required and a variety of other criteria. This is likely to lead quickly to a search for service providers that specialize in this sort of analysis and/or for software that can organize the effort.

Once organized, Internet Monitoring can assist in the identification of websites selling products and the correlation of sales with an indication of fraudulent or illegitimate activity. More advanced capabilities can identify additional data points useful in quantifying threat associated with a particular site, and/or associating the site with larger affiliate networks. An Internet Monitoring program should provide meaningful intelligence about sellers that can be used to assess risk, support further investigations, enforce actions, and other protection initiatives for brand/product.

As summarized above, it is useful to begin any Internet Monitoring program with basic threat risk assessment and to align the Internet Monitoring program with the company's internal business strategies.

Some general areas of discussion are:

- **Probability:**
  - Likelihood of being illicitly traded on certain marketplaces and/or websites
  - Exposure within the Business-to-Business (B2B) marketplaces, Business-to-Consumer (B2C), Consumer-to-Consumer (C2C) and/or the trade boards
- **Risk:**
  - Product risk assessment specifically around areas of exposure/risks as it relates to the Internet behaviors
    - Product category, Usage/Dosage Requirements, Packaging or Dispensing, Supply Chain, product life cycle, etc..
- **Knowledge:**
  - Consumers knowingly buying counterfeit product

One approach might be to target business-to-business or trade board sites for monitoring of a company's products being offered for sale. This approach can produces large sets of data that must be reviewed to identify and prioritize possible targets for further investigation or covert test purchases. Also because many trade boards will honor requests to take down offers to sell prescription medicines, this can be an effective first step toward control of the problem. This is often utilized in identifying targets infringing on a company's trademark for enforcement actions, such as Cease and Desist letters, domain registrar/registrant take-downs, and other civil actions that can disrupt the rogue organization.

A complimentary approach utilizes an experienced investigative consultant to create a pre-text or covert website posing as a trader who buys and sells pharmaceuticals (none are actually sold). This approach often allows for the investigator to "engage" with the illicit pharmaceuticals traders at a higher level in the criminal organization. This approach should not be undertaken without a review by the company's legal department or outside counsel.

There are several suppliers that provide Internet Monitoring capabilities for a Secure Supply Chain – Internet Monitoring program. While the suppliers utilize various techniques and approaches, most of the solutions provide the same basic capabilities of scanning and storing data from the various Internet sources. However, each offers different approaches of classifying, analyzing, discovering threats/patterns, and isolating/prioritizing targets. Some suppliers have invested significantly into the automation in the form of an advanced software architecture, others have invested in the human analytically capabilities, and others have developed a 'balanced' approach to technology and human analytics.

Other software packages can assist in the Internet monitoring of pharmacy websites. This software can assist in vetting if the Internet pharmacy is accredited by a recognized authority, identifying aliases of an illegal website, identification of unusual product pricing as well as trademark infringement. This information can assist companies in their process for serving cease and desist letters to domain name service providers hosting the illegal website. Monitoring social sites, blogs, trade boards and other Internet communities relative to a company's products may also identify data relative to threats and signals.

The implementation of any Internet Monitoring program (especially if the company begins an active enforcement program) requires a certain degree of knowledge and experience in these specialized investigations as well as the assistance of experienced, trusted and well vetted outside consultants with proven capabilities to conduct investigations of pharmaceutical illicit trade operations. While not mandatory, prior law enforcement experience of product security unit members is considered highly desirable as both complex legal and operational issues are likely in conducting and coordinating these types of investigations. Finally, because these investigations require extensive use of outside consultants/vendors, sufficient budgetary funding is required in order to sustain an effective program.

The information that is discovered during the Internet Monitoring program should become a source within the 'Database of Threats and Signals' previously mentioned.

Monitoring of Physical Operations

The discovery and monitoring of grey/black market physical drug selling operations (sometimes referred to as *brick-and-mortar operations)* is one of several product security investigative tools that a manufacturer can utilize to effectively identify potential pharmaceutical illicit trade operations. This proactive technique can be useful in identifying rogue/illegitimate sellers of CUDD product. This includes the use of scanning and investigative tools to identify organizations or individuals offering CUDD product, and may also involve the design and execution of targeted market surveys. The purpose of these investigative activities is to develop meaningful and actionable intelligence regarding rogue drug sellers which also can be useful in assessing product risk. Information and evidence gathered utilizing this technique is used to initiate further investigations, referrals to law enforcement for possible enforcement action, as well as other brand/product protection initiatives.

So-called brick and mortar sellers, once identified and located, can also be targeted for face-to-face meetings with investigative consultants, posing as buyers or dealers, in an effort to gain inside intelligence about the rogue operation and/or make hand-to-hand purchases of illicit products. This approach, while

potentially extremely productive, should be carefully planned due to possible safety risks and should not be undertaken without a review by the company's legal department or outside counsel. Furthermore, the involvement of law enforcement in this investigative scenario is strongly recommended.

Leveraging Existing Internal Systems and Processes

Pharmaceutical manufactures generally maintain a set of existing processes, many related to GMP functions, that lend themselves naturally to being extended as input signal generators for counterfeiting and diversion attacks. Companies should link their Complaints, Returns and other existing process signal acquisition to its CUDD analysis process

Complaints

The company's complaint handling system is a way to receive information from customers on potential counterfeit, diverted or tampered product. Companies should determine what the indicators of a potential counterfeit product may be based on their products and incorporate them into their operating procedures. Based on the type of complaint handling system that is used, the product security group should be notified of issues through the system or manually based on operating procedures.

Adverse Events

Patient and health professional reporting of adverse events is another way to discover information on potential CUDD product. Companies should determine what types of adverse events should be evaluated as potential counterfeit. Other items to look at in adverse event reports may be "buzz" words, which may indicate potential issues due to risks. Words such as "purchased on the internet" or "imported" may indicate risk. Patients or health professionals may even state they think their product is counterfeit. Based on the systems used by the company, the product security group should be notified of issues through the system or manually based on operating procedures.

Returns

Product that has been returned by customers has the potential to be CUDD product as returned products have been out of the supply chain that is visible to the manufacturer, and substitution or tampering may have occurred. Individuals engaged in CUDD activities look for opportunities to gain credit/revenue through the abuse of the product returns by returning non-genuine products or tampered products (re-labeling to change expiration and lot number). To deter this threat, enterprises should incorporate product authentication abilities into the returns process such as cross checking the product with the lot number and expiration date and look for abnormality in the returns data (e.g., returned more product than what was sold, weight of the returned product).

In addition, if a company's return policy is to destroy returned product, then they should review the "Product and Material Destruction" section below. If the policy is that returns could re-enter the market place, multiple checks and processes need to be in place to ensure that the product is authentic, as well as ensuring other quality aspects of the product.

Wholesaler Audits

In many cases, the wholesaler is the first paying customer for a pharmaceutical firm. Although the product is owned by the wholesaler, the pharmaceutical company should still play an active role in ensuring the patient receives a safe and quality product. The frequency and depth of wholesaler audits vary due to the

fact they are the legal owner and contractual agreements between the wholesaler and the pharmaceutical company may not allow for in-depth audits. At a minimum, when auditing a wholesaler one should include both a review of their procedures/practices and a physical inspection of a warehouse. It may not be practical to visit all the wholesaler locations but understanding the corporate security practices would provide a good foundation. Additionally, a physical inspection of their warehouses could provide support that the procedures are put into practice. Previously performed product risk assessments can be used to provide a risk-based approach to audits.

Note: Reconciliation of the quantity of product purchased from the pharmaceutical company with the wholesaler sales and inventory records is a best practice.

Quality Audits

A quality audit is typically a formal review of quality practices of third party suppliers, e.g., contract manufacturers, and third party logistic providers. An audit is performed by a person trained in the quality requirements of the product and the associated Quality Agreements. A typical quality audit inspects the physical environment for deviations from the company and regulatory expectations and reviews operational procedures against the same standards. Finally, supplier practices are compared against the procedures to ensure the operations are within guidelines. Any deviations from company or regulatory guidelines are documented and a plan to close the gaps is expected. Quality Audits are an opportunity to ensure that third party suppliers are supporting brand protection requirements for detection of CUDD products.

Call Center

A pharmaceutical company typically establishes a call center to receive/answer specific product questions and complaints. A call center can be a very effective avenue for a company to gain feedback from its customers. Call center staff should be trained on the companies' policies and procedures relative to how to handle and triage any critical call on counterfeit, tampering and Internet purchase.

Authorized Distributor of Record

A pharmaceutical company will typically have a written agreement in place with its authorized distributors of record (ADR). It is good practice to require distributors to buy products directly and only from the manufacturer. This can limit stolen or diverted product from re-entering the distribution channel. Buying from an ADR helps to ensure retail (and smaller distributors) that the purchased product is authentic. These lists of ADRs are made public by the pharmaceutical companies in an effort to further strengthen the integrity of the distribution channel and posted on their company's Internet site as a best practice.

Product and Material Destruction

Product which is damaged (beyond acceptable limits) during production or distribution should be destroyed. The quality organization should assess the impact of product damage and there should be procedures on product destruction. Care should be taken when destroying product to ensure the entire quantity undergoes destruction and cannot make its way back into legitimate distribution channel. An inventory count should be part of the destruction documentation as well as a thorough security assessment into the firm performing the operation. Additionally, the transportation to the destruction site should be secure.

Product Analysis

Pharmaceutical companies routinely perform product analysis on suspected counterfeit or diverted product obtained in the marketplace to confirm its authenticity. This testing may be performed in conjunction with law enforcement agencies who are working to confirm whether the product is the manufacturer's genuine product. This testing may include lab assays to determine the chemical make-up/fingerprint and/or inspection of the packaging components and labeling including any overt or covert product packaging protection features (e.g., holograms, light shifting ink, microtext, invisible markers) applied by the original manufacturer.

Product Sales Analysis

In the United States there is a real opportunity to use analysis of syndicated and proprietary sales data to identify certain forms of product diversion due to the advanced state of these data products. The various data products document drug sales into and out of entities in the supply chain from the manufacturer down to the patient and can support the analysis when used in combination. Such data products may include manufacturer direct sales, charge backs, EDI 852 inventory data, EDI 867 sales data, IMS HEALTH DDD and WK HEALTH Source Non-Retail sales data, Medicaid rebate data, medical claims data, insurance eligibility verification data, and institutional diagnosis and procedure data. Careful consideration should be given in the selection process of the data products in the analysis, because of the limitations of these products.

The basic premise in this analysis is that sales into an entity must closely approximate sales out of that entity. And although there are legitimate reasons why deviations from this formula should exist in some cases, there are clear and undisputed reasons why they should not in other cases. It should be noted here that due to imperfections in the data, it is impossible to discover every case of diversion; however, the data is significant enough to answer the question whether a product is diverted, provide a measure for the degree of diversion, and identify a significant number of diversion cases in most therapeutic areas. Please note that this type of analysis may not be possible in other countries, including countries in Europe, due to lack of data availability, or significantly lower data completeness.

Product Security Features and Serialization

Security features (i.e., overt and covert features that by their presence help to confirm the genuine nature of the product and packaging), anti-tamper features and serialization (the unique numbering of individual units of medicine) offer opportunities to support monitoring for CUDD products. This document will not go into depth on any of these tools but rather recognizes the importance of these tools as part of a complete monitoring and detection program.

A company should define a strategy around the use of product security/anti-counterfeiting technology features. Security features can play an important role in identifying if a questioned product is genuine or not, and can be particularly useful in a field setting, where laboratory analysis is impossible. For example, these technology tools can be integrated into the processes for special market assessments such as Internet buys or wholesaler/distributor audits. The strategy should be supported with processes and training of the resources that will be called on to draw inferences from the inspection and analysis of security features.

Serialization is an emerging overt feature that can be implemented to authenticate a pharmaceutical package. In time, it should assist companies in verifying the chain of custody and ownership throughout

the supply chain and provide for direct package authentication, if supporting business processes are in place.

As an additional part of a company's strategy, there is increasing usage of hand-held analytical tools to rapidly test and identify if the physical product is authentic or not. Considerations of where it should be used (e.g., in the lab or the field), and how it may direct the investigative path of an incident need to be defined. There may also be other inherent product characteristics/properties (e.g., impurities) that through analytical technology can be used to authenticate the physical product.

There are limitations on all of the above security technologies and it is the responsibility of the company to understand these limitations and to have appropriate controls and systems in place to manage them.

Communication and Education

The importance of communication and awareness to detect and prevent illicit trading of pharmaceuticals cannot be overstated. Companies should have a process for educating their supply chain partners, both internally and externally, about signs of potential illicit activity that should be reported to the manufacturer and health authorities and the procedure to report.

Internal Communication and Education

It is important that internal resources are aware of the existence of CUDD risks an how to report concerns to the company's Signal Data Base (see above). It is also critical to engage/train company stakeholders more completely on specific processes that relate to their CUDD responsibilities for monitoring. These steps facilitate quicker recognition of potential illicit activity and early detection and remediation. Below are examples of useful techniques.

- A Product Security/Protection website on the company's intranet for the posting of awareness material, alerts and related content
- Training of returns management on authenticating returned product
- Educating the field sales force on signs for diversion and counterfeiting (e.g., visual inspection of product for authenticity and correct country of origin; monitoring of sales data for irregularities)
- Training of complaints and call center staff on CUDD processes
- Establishing reporting mechanisms can serve as an effective tool for early detection and prevention.

External Communication and Education

A manufacturer's supply chain potentially has access to a range of signals that can provide early warnings about potential CUDD activities.

- Wholesalers receive inquiries from their customers about suspicious activity
- Pharmacies/clinics approached by questionable sellers about "great deals" on medicines

It is also important to work closely with QA components to ensure their awareness of the problem and to frequently communicate on possible issues identified during QA audits of external Supply Chain partners and stakeholders. Furthermore, there should be a reporting procedure in place for lost or missing product incidents involving wholesalers and distributors that require follow-up investigation. Experience has

shown that these losses can add up to large sums over time and are sometimes an indication of a systemic problem with a supply chain partner.

Educating the public should also be considered as a form of external communication to raise the public's awareness of this issue. This can be accomplished by using the company's website for topics such as:

- The dangers of pharmaceutical counterfeiting and diversion and specific incidents
- Buying pharmaceutical products from entities outside the legitimate supply chain (i.e., Internet pharmacies)

The above strategies can easily be developed and implemented by a pharmaceutical manufacturer and are considered an important component of a best practice, multi-prong approach to product protection.

Working with Outside Agencies

Outside law enforcement, regulatory and pharmaceutical industry product security organizations potentially have valuable information on rogue actors, their affiliations and practices. Companies should have a process for two-way communication of information with these outside organizations. Specifically, companies should have processes for organizing and sharing the results of their internal investigations with these entities, as well as processes for reaching out to these organizations to inquire about specific individuals or illicit traders that pose a potential CUDD threat to the company's products and patients.

As an example of some of the originations the companies should consider reaching out to are:

- US FDA: http://www.fda.gov/Drugs/ResourcesForYou/Consumers/BuyingUsingMedicineSafely/CounterfeitMedicine/default.htm
- MHRA: http://www.mhra.gov.uk/Safetyinformation/Generalsafetyinformationandadvice/Adviceandinformationforconsumers/Counterfeitmedicinesanddevices/index.htm
- EU Tax and Customs Organization: ttp://ec.europa.eu/taxation_customs/customs/customs_controls/counterfeit_piracy/index_en.htm
- INTERPOL http://www.interpol.int/XLKeZ/Public/FinancialCrime/IntellectualProperty/Default.asp
  US Department of Justice CCIPS: http://www.justice.gov/criminal/cybercrime/

Test Purchase Capabilities

Undercover test purchases are a necessary step in the process of confirming a CUDD incident within an investigation. While prior intelligence gathering or initial phases of an investigation may indicate counterfeit or other fraudulent events are occurring, it is the actual purchase and delivery of product that verifies this threat and provides substantive evidence to support further enforcement actions. As such, it is often critical for companies to be able to acquire products from the marketplace, whether it be wholesalers, online traders or websites, brick-and-mortar pharmacies, or other pharmaceutical outlets. Assuming such a purchase is in order to support an ongoing investigation into suspected fraudulent actions, it is necessary for these purchases to be made under pretext such that the seller is not aware of the investigative nature of the purchase.

This capability, however, should be approached with extreme professional due diligence and robust controls in place. Ethics and legal regulations and local laws need to be well understood. Additionally, proper documentation and chain of custody procedures need to be followed in order for purchased products to support further enforcement actions.

An undercover test purchase usually involves making a purchase of the product of interest through some covert means (so as not to disclose the company's investigation of the target). Companies should have a process for initiating, managing and analyzing test purchases, paying attention to any legal constraints as well as the effective acquisition of test products. It is important to maintain strict chain of custody for each sample, as well as documented evidence on the website or location from which it was purchased, and documentation of the financial transaction. After obtaining products through test purchases, it is necessary to perform an analysis of the product to determine if it is counterfeit, diverted, or in any other way fraudulent.

There are several suppliers that provide test purchasing capabilities. While there are some standard capabilities and approaches when performing a specific 'test purchase', the geographic reach and services around this capability vary greatly. Some suppliers have a large presence in many countries, and some suppliers provide lab services to analyze the product, and some approach it from an 'investigator' / security perspective. Companies need to develop a tactical plan for how they want to approach each purchase and ideally before they execute the purchase know what their plans are for the results.

Undercover test purchase capabilities should be a part of a larger Product Security program. In order to maximize the benefit of test purchases, a robust intelligence gathering and data collection effort is needed to appropriately identify targets for test purchases. This targeting should be based on the relative threat associated with a particular seller, the likelihood of gaining meaningful information as the result of a test purchase, and the likelihood of conducting meaningful enforcement actions against an entity if fraudulent activity is detected as a result of the test purchase. In addition, samples obtained from the test purchases need to be analyzed to determine if they are counterfeit, diverted, or otherwise fraudulent. The summation of intelligence gathered during the targeting, purchasing, and product analysis, can then be compiled into an enforcement package for hand-off to law enforcement agencies for criminal enforcement, or corporate attorneys for civil enforcement.

Incident Management

It is important for a company to identify the leadership of and establish inter-company links for incident management and reporting. In general, companies should have a written process defining roles and responsibilities, decision rights and steps to be followed during an incident. This enables the appropriate functions within a company to engage at the immediate local market level to resolve the current CUDD issue, and to monitor the broader picture of incidents collectively for continuous improvements to product and supply chain security. For example, a diverted product could indicate that theft occurred in a particular market signaling that security should be notified to investigate the distribution and supply chain flow to identify what gaps there are to mitigate in order to prevent additional theft.

Reporting of Incidents

There is both an immediate need to communicate local market incidents and also to collectively assess all incidents for continual improvement actions that a company may take to further patient safety and to secure their products and their supply chains.

Most companies have an existing business process that assesses product quality issues and escalates them up to a product recall committee/team as needed. These committees/teams typically include the functions of Quality, Supply Chain, Commercial, Medical Affairs, Regulatory and Legal departments. By extending the committee/team to include Security and Toxicology, as needed, for counterfeit and tampering incidents, the company can make immediate decisions for obtaining additional insights into the local market situation for this type of activity; in determining patient safety risk/impact and communications to the public or healthcare providers as well as communications to and interactions with the local health authorities.

Companies should also have a corporate management committee--a team responsible for the periodic assessment of its collective incident data-- so that investments in technologies and the supporting business processes can be agreed upon for further improvements to the protect the product and its supply chain. This corporate management committee/team should include the head of Quality, Supply Chain, Manufacturing (including Packaging), Commercial, Security and Legal.

What Needs to be Communicated and How to Communicate

For companies to take appropriate actions and assign resources effectively for incident management and market monitoring, the type of incidents should be tracked, trended and reported out on a periodic basis. This approach provides data in a standardized, consistent manner for communicating among various company functions, visibility into the magnitude of the company's issues, and facilitates discussions around the issues as to what should be done.

At a minimum, the types of incidents - counterfeit, tampering, diversion, unapproved - should be differentiated and tracked as a company's actions/response may be different depending on the incident type. Additionally, these data attributes should be collected:

- Which country/geographic location
- Where in the supply chain the discovery of the incident was originally made
    - Consumer
    - Doctor
    - Clinical setting
    - Pharmacy
    - Law enforcement raid
- How it was observed, i.e., what made it suspect
- Who reported the incident to the company

Conclusion

The distribution and sales of Counterfeit, Unapproved and Diverted Drugs (CUDD) are a global concern for pharmaceutical patients, healthcare providers, regulators and manufacturers. This document has provided a general overview of the definitions, sources, and distribution of CUDDs in the finished form, as well as a high level summary of Supply Chain Security (SCS) monitoring practices and tools that pharmaceutical companies can use to help detect, deter, and to establish appropriate control for CUDDs in the supply chain. This document was meant to provide a basic understanding but does not seek to provide detailed guidance.

Appendix A – Checklist of Monitoring Programs/Techniques

	Requirement	*Reference*
1.0 Definitions		
Product Characteristics		
a.	Adopt or develop company definitions for Counterfeit, Diverted and Unapproved Product	
Distribution Channels		
a.	Understand the different distribution channels of which Counterfeit, Diverted and Unapproved Product. A primary channel is the Internet through 1) B2C pharmacies, 2) B2B trade board and 3) Consumer exchanges.	
Monitoring Practices		
a.	Develop Product Security Threat Risk Assessment A basic approach to developing a Product Security Threat Risk Matrix is to review the relative likelihood or "desirability" of the criminal creation and insertion into the legitimate supply chain of CUDD. Possible parameters to consider could include: • Risk of therapeutic class (e.g. Acute pain medicines are less likely to be counterfeited that more chronic treatments.) • Pricing (e.g., high value) • History of past CUDD for Product/Therapeutic Class • Supply chain handling/transportation • Price differentials (International pricing, discount structures) • Pricing Reimbursement Structure • Form of product (solid v. injectable)	
b.	Threat and Signal Intelligence System – database to store and analyze threats and signals collected from the various components	
c.	Theft Monitoring and Analysis	
d.	Internet Monitoring – searching for sites/marketplaces on the Internet which are attempting to sell illegitimate product	
e.	Monitoring Physical Operations – use targeted market surveys to locate physical locations attempting to sell Counterfeit, Diverted and Unapproved Product.	
f.	Existing Internal Systems - many related GMP functions lend themselves naturally to being extended as input signal generators for counterfeiting and diversion attacks. • Complaints • Adverse Events • Returns • Wholesaler Audits • Quality Audits • Call Center • Authorized Distributor of Record	

	• Product Destruction • Product Analysis	
g.	Product Security Features – multi-layered strategy should include a range of overt, covert and forensic technologies • Packaging/labeling product security features including tamper evident features • Product properties and features	
h.	Communication - Internal • A Product Security/Protection website on the company's intranet for the posting of awareness material, alerts and related content. • Educating the field sales force on signs of diversion by clinics and doctors	
i.	Communication - External • Wholesalers receive inquiries from their customers about suspicious activity • Pharmacies/clinics approached by questionable sellers about "great deals" on medicines • Monitoring sales data from wholesaler to direct customers (EDI 852, EDI 867) • Public education on the dangers of pharmaceutical counterfeiting and diversion and specific incidents and buying pharmaceutical products from entities outside the legitimate supply chain (i.e., Internet pharmacies)	
j.	Working with outside agencies • Law enforcement – providing details on internal investigations and obtaining information on external investigations • Training Customs and other authorities on your products and the specific security features	
k.	Undercover Test Purchases – purchase of product of interest through covert means. • Process for initiating, managing and analyzing test purchases • Legal constraints • Maintain strict chain of custody • Documented evidence of the website or location of purchase • Perform analysis of the product to determine if it is counterfeit, diverted, or in any other way fraudulent.	
l.	Incident Management • Data collection – 1) Region, 2) Where in the supply chain [Consumer, Doctor, Clinical setting, Pharmacy, Law enforcement], 3) Who reported and how was it observed • Communication plan for incidents • Collect, analyze and trend incidents over time • Governance process and escalation	