VERIFY BRAND

Protecting People
Protecting Brands

Verify Brand Response to Questions and Comments to the FDA Regarding Anti-Counterfeiting Initiatives

Comments to Docket No. 2005N-0510

2/23/06

7277 Boone Avenue North Minneapolis, MN 55428-1519
763 235 1400 Phone 763 235 1401 Fax

1. **Obstacles to widespread use of RFID technology:**
   a. **RFID Tag Economics**
   b. **RFID Standards**
   c. **RFID Privacy Concerns**

RFID Tag Economics:

RFID readers and related software are not a significant part of the ongoing costs of using RFID technology. Costs associated with individual tags are very significant and are estimated to remain so for a considerable period of time. Based on the experience of our parent company, a manufacturer of RFID tags, (http://www.meyersconverting.com/rfid/) we suggest the FDA consider the process of making finished RFID tags or labels to be made up of essentially three layers.

- The first layer is making the large silicon wafers. Each wafer contains many, many silicon RFID chips. Although there is significant sunk capital costs in such fabrication capability, there is a robust capacity for this wafer production and the needed economics are well understood and are not projected to be a source of future cost difficulties.

- The second, or middle, layer involves taking wafers and removing from them the grain of salt size individual RFID chips and accurately attaching them (registering them) to a given antenna structure on a label or tag. The necessary economics will not be achieved until this process is commoditized in much the same manner as high quality litho printing has been commoditized. That is, very low cost organizations (typical of the current suppliers of pharmaceutical tags and labels) buy highly engineered and refined equipment (that is certain to work well because wrong engineering approach machinery, or poorly executed machinery has been driven out of the market place) depreciate it over a period of time and then reduce prices to fill excess capacity. The machinery (processes) in place today for this middle ply is anything but highly engineered, refined and depreciated. Much of the equipment in use has been custom built by the user. (Imagine what printing would cost if printers made their own presses.) We estimate it will be between five and ten years before this will take place.

- The third layer, is the making of the finished tag or label including the printing (foil stamping etc.) of the required antenna. There is already a very robust and competitive capacity for this type of production; it is not a source of the economic problem.

RFID Standards:

There are a number of open standards issues which were discussed at the public workshop. Obviously, such standards are necessary for widespread RFID implementation. We believe these standards will be achieved before the volume production economics and therefore, standards, while critical, are not the pacing issue. We are an active participant in EPCglobal and recommend that the FDA continue its support of the organization in general and the serialization committees in particular through participation and guidance.

We have specific recommendations and rationale with respect to open standards issues; however, we believe a review here is beyond the scope of this submission. Please let us know if you would like to discuss these matters further.

RFID Privacy:

We, and the leadership of EPCglobal, believe that privacy is a very serious concern. Unaddressed, or poorly addressed, it has the potential to indefinitely suspend the opportunity held out by RFID.

We have yet to see an electronic or mechanical solution that we believe will be accepted by the marketplace. While kill bits and mechanical disablement are technically valid approaches they bring with them both significant economic concerns and, in any event, will be considered to be insufficient by privacy advocates as the required "kill" process step will be perceived as being too easily bypassed.

We strongly endorse the use of "Content Free" (a.k.a. inherently confidential) serialization approaches. It is clearly workable from a technology standpoint with thousands of implementations of the proven "web services model" allowing any authorized user to rapidly bring up and apply any information they would have otherwise wished to have been written in the tag.

A less robust or less certain approach not only endangers the RFID opportunity; it would make necessary warnings on the package and or label that would be pointless (or at the very least temporary and de minimis) in a content free numbering system. Given the critical need for patient information on very limited package and label real estate we urge the FDA to consider a "content free" serialization approach because it will minimize, if not eliminate, the need for RFID warnings and is by its very nature, confidential.

Concluding RFID Comment:

In general, we see the RFID tag simply as a more efficient number carrier. Mass serialization is already being accomplished with 2D bar codes and even human readable codes. While there is no doubt that, some day, the RFID tags will make the supply chain more efficient, we don't believe economic incentives to drive efficiency are properly part of primary FDA mandate with respect to protecting the public health by assuring safety, efficacy, and security. While we do see that an argument can be made for RFID incentives being within the purview of the FDA's secondary mandate to make medicine and foods more affordable, we think a very poor or even negative Return On Investment is a likely outcome if the market is not allowed to go through the iterative process (make, try, keep or reject) of developing a robust and low cost manufacturing base. Further, as pointed out in The Los Alamos National Laboratory Anti-Counterfeiting Study (see **Attachment A**), focusing on a transaction technology, such as RFID, takes away from a focus on product authentication where the greatest opportunity for thwarting counterfeiting and diversion really lies.

2. Mass Serialization Issues:

a. **Numbering Conventions**
b. **Timetable for Widespread Use**

Mass Serialization Numbering Conventions:

Verify Brand, along with The Los Alamos National Laboratories, urges the use of random numbers for mass serialization. As stated before, random numbers are inherently content free, eliminating privacy concerns. Much more importantly, when combined with web authentication, they are the single most effective anti-counterfeit technology. In practice, an incredibly minute subset of the available number combinations is actually applied to a product. For instance, fifty million numbers taken out of a 12 digit alphanumeric code represent less than .000000000001% of the available numbers. And, of course, counterfeiters need many, often hundreds, and even tens of thousands, of correct numbers for their products. Since any number of databases (each can be at its own I.P. address) can be used, there is essentially an infinite number of numbers available for use. Further, since numbers entered more than a set limit (such as three times) can be shown to be no longer valid, simply stealing valid numbers from existing packages does not defeat the approach. In effect, these numbers are like snowflakes or fingerprints and can be associated with the individual products and with any other information as authorized and as needed. Of course, these numbers can be carried by RFID, 2D or linear bar codes, human readable text, and any number of other proprietary or non-proprietary methods.

Verify Brand urges the FDA to give guidance to use alphanumeric codes in mass serialization. While there is no advantage to an alphanumeric code in digital form, in the event a human readable code is desired, alpha numeric codes take up much less package or label space and are easier for humans to enter in computer systems.

Verify Brand urges the FDA to give guidance to provide human readable codes both as back up to the RFID, 2D bar code or other method and to provide the consumer with the tools to protect themselves. In addition to a back up capability in the supply chain, human readable codes will allow individual consumers to be the “many points of authentication”. The intuitive nature of this seemingly random checking could well turn out to be one of the most effective tools in quickly discovering instances of counterfeit or diverted products.

Verify Brand urges the FDA to give guidance to not use vowels in the use of alphanumeric codes. The use of vowels is not necessary to achieve the volume of codes necessary to be effective and creates an ever growing risk or randomly producing a code whose human readable version is vulgar or insulting. While filtering for offensive words is a legitimate option, we recommend the simpler no vowel approach common in gaming applications.

Mass Serialization Time Table for Widespread Use:

Verify Brand is already underway with a number of pilot projects and validated, (i.e. operating in FDA inspected facilities, solution compliant with FDA guidance 21 CFR Part 11, 808, 812, 820 and compliant with FDA’s QSR and General Principles of Software Validation) live in the field mass serialization. Our non disclosure agreements do not allow for the sharing of specifics in a public forum, however, we can say our Fortune 50 size clients are accelerating their programs because of the additional

benefits beyond anti-counterfeit protection in the areas of unauthorized product returns and product diversion. Combined with very, very low costs and already existing ability to make the necessary 2D bar codes (and human readable text) through modern ink jet technology even very large companies can complete their mass serialization project in a twelve to eighteen month time frame from its inception. No new technology is required to start, nor is there any "on the horizon" technology that would invalidate the investment in an immediate serialization effort. Further, the disciplines necessary to uniquely mark each product are the "crawl" in a crawl, walk, run strategy that will one day lead to greater automation through an EPCglobal-compliant RFID-based system.

We have experienced that mass serialization is definitely a top down led effort. Although putting unique numbers on each package is relatively simple in theory, in practice, it touches so many parts of the organization that it requires leadership from the most senior parts of the organization; lacking this leadership, project implementations stall indefinitely. In this regard, the FDA's continuing efforts to give guidance and highlight the many advantages of mass serialization are particularly welcome.

3. Data Management and Data Security
- **a. Distributed Systems**
- **b. Data Management and Security Standards**

Distributed Systems for E-pedigree and Mass Serialization:

Verify Brand strongly suggests a distributed system for storing and exchanging e-pedigrees and managing and authenticating mass serialization. This system allows for better performance, scalability, and flexibility. In effect you are leveraging the power of the architecture of the Internet. In addition, the standards forced by Internet use will enable a company which has their own system for managing pedigrees and serialization to integrate it with other enterprise applications, boosting the value of the system.

Data Management and Security for E-Pedigree and Mass Serialization:

In addition to digital signatures on the pedigree documents, we suggest data exchanges should be encrypted with digital certificates to prevent the theft of the pedigree data. This method supports the distributed approach to storing pedigrees. In addition to digital signatures, role based permissions should be used to grant users access to only the parts of the system necessary for them to perform their task. All verification, authentication, and reporting should be transmitted over Secure Socket Layers (SSL) to provide theft of pedigree data. SSL technology is a highly secure and widely deployed technology.

In addition to guidance such as 21 CFR Part 11 and FDA's General Principles of Software Validation, standards as documented in ISO/ICE such as 17799 or 12207 should be considered to assure compliance to acceptable standards

Finally, an independent audit of a level such as SysTrust SAS Type I and Type II should be recommended. Such an audit requires an entity to meet high standards for the protection of the system

components from unauthorized access, both logical and physical. The criterion includes requirements that the entity:

- Has effective security policies,
- Discloses its key security practices,
- Uses procedures to achieve its documented system security
- Objectives in accordance with its defined policies, and
- Have controls to ensure that these policies are followed.

4. Issues Related to adoption of e-Pedigrees

a. General Comments on the role of e-Pedigree
b. Concerns regarding the "Substitution Flaw" in e-Pedigree
c. Paper and e-Pedigrees coexisting (Human Readability)

General Comments on the role of e-Pedigree

Verify Brand is a service supplier to the Health and Life Science industries in the area of anti-counterfeit and diversion protection through the implementation of e-Pedigree and Mass Serialization Solutions. We have noted confusion in the marketplace with respect to the role and capabilities of these strategies. Pedigrees, including electronic versions, seek only to authenticate transactions rather than products. In general, we believe the FDA was wise to delay e-Pedigree regulations with respect to the PDMA in anticipation of Mass Serialization. Although confidence in the near term widespread use of RFID technology was misplaced, this neither invalidates the powerful benefits of Mass Serialization nor suggests there is any reason for delays to continue as long as near term and widespread use of RFID as the only number carrier is not a requirement. We fear an outcome in which those who have been disappointed in RFID adoption rates will grasp at e-Pedigree and, in effect, attempt to force this useful tool to do more than it is inherently suited to accomplish. In other words, the original idea of forcing the many smaller or secondary distributors to document the chain of transactions was a good one because making the participants more monitored makes one area of exposure safer. Automating this process through the use of electronics and public key infrastructure (digital signatures) makes the Pedigree tool more effective and efficient. As presently conceived, say in the Florida implementation model, e-Pedigree is still only a (very good) tool for monitoring and authenticating transactions. The FDA should be wary of proponents seeking the expansion of any one system or tool. We urge the FDA to work with the various state governments to help create a standard for e-Pedigree for the sake of interoperability and efficiency in the system. We urge the FDA to take the time necessary to help set this standard correctly.

Concerns regarding the "Substitution Flaw" in e-Pedigree

When product serial numbers are not required to be part of an e-Pedigree, the system is left open to an unscrupulous wholesaler taking in authentic product (along with an authentic pedigree) and then also taking in a similar quantity of counterfeit drugs. Counterfeit drugs in this example could be sold with an authentic pedigree. Product serial numbers should be part of the eventual pedigree mandate to eliminate this potential opening.

Paper and e-Pedigree system coexisting (Human Readability)

As a practical matter we don't envision the possibility of these two systems not coexisting for at least some period of time. Requiring a printable or human readable version of the e-Pedigree would support a coexistence period. Of course, the nature of digital signatures is such that they are not printable in a literal sense, therefore guidance in this regard would need to stipulate that printed versions of e-Pedigrees be water marked with a clear violator indicating "uncontrolled copy".

Attachment A

LAUR-04-0855

An Anti-Counterfeiting Strategy Using Numeric Tokens

Los Alamos National Laboratory

Vulnerability Assessment Team
Roger G. Johnston, Ph.D., CPP*

MS J565, Los Alamos, NM 87545 USA
phone: 505-667-7414, fax: 505-665-4631
email: rogerj@lanl.gov

* Head of the Vulnerability Assessment Team at Los Alamos National Laboratory.

Abstract:

Introduction: The counterfeiting of pharmaceuticals continues to be a major worldwide problem, with serious public health and economic consequences. In theory, anti-counterfeiting tags could help to solve this problem. Unfortunately, there are currently no practical, effective tags that cannot be easily counterfeited. Method: This paper discusses a different, relatively low-tech and low-cost approach called the “Call-in the Numeric Token” (CNT) technique. It relies on participation by pharmaceutical customers (possibly including consumers). They check, via phone or Internet, on the validity of the unique, random, unpredictable identity (ID) number assigned to each pharmaceutical container they possess. The numerical container ID is a virtual tag or token, rather than a physical one that is susceptible to counterfeiting. Counterfeiters are hampered by being unable to guess valid IDs, by being unable to easily acquire large numbers of existing valid IDs, and by being detected when multiple customers report the same IDs. Results: At least some counterfeits can be detected even if only a small percentage of customers participate. The technique is particularly well suited for single-dose (“unit of use”) packaging, but can otherwise be adapted and automated for resellers, wholesalers, repackagers, and other high-volume customers. Conclusion: While it will not absolutely end counterfeiting, CNT can make pharmaceutical counterfeiting easier to detect and study, and more difficult for counterfeiters.

Introduction

Counterfeit pharmaceuticals continue to be a major problem, with serious medical and economic consequences.[1-6] In theory, high-tech tags placed on packaging, or taggants doped into the product, could be used to authenticate pharmaceuticals and other medical products. (A "tag" is a device or feature that uniquely identifies an object or container. A "taggant" is a trace chemical added to a product to give it a unique "fingerprint".)

To be practical, tags or taggants need to be (1) inexpensive, (2) difficult and/or expensive to counterfeit, and (3) quick and easy for non-technical personnel to verify. In practice, such tags or taggants do not currently exist.[7-10] They may not even be possible.[7-9] Indeed, according to the FDA, "All anti-counterfeiting technologies can be defeated."[6] This statement is certainly consistent with our experiences in the Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory.[11-13]

Inventors, manufacturers, and vendors of anti-counterfeiting tags often claim to have a unique manufacturing process that nobody else can duplicate. In our experience in the VAT, this is usually untrue. Moreover, one factor often overlooked in discussions about anti-counterfeiting tags is the fact that a tag (and its real performance) does not actually need to be counterfeited for an adversary to be successful. Instead, only the superficial appearance and <u>apparent</u> performance of the tag usually needs to be mimicked. This is much easier.

Clandestine taggants, or covert tags such as secret inks[14] and surreptitious packaging marks[6,10,14-16] appear to be particularly impractical, especially for use by individual consumers. Moreover, they require keeping secrets—not a viable long-term security strategy for consumer products. Besides, the trace contaminants in pharmaceuticals already serve as a unique, hard to counterfeit "fingerprint" that can be analyzed in a laboratory, though at great cost.

Passive radio frequency transponders (RFIDs) or memory contact buttons are another common suggestion for anti-counterfeiting tags[6,14-16], but we in the VAT have demonstrated that they can be cheaply and easily counterfeited.[11,12,17]

This paper discusses an alternative anti-counterfeiting technique that does not require high-tech or covert tags or taggants. While imperfect, it nevertheless offers the possibility of at least partially detecting counterfeits and impeding counterfeiters at relatively modest cost. This strategy, termed the "Call-In the Numeric Token" (CNT) technique, would also be applicable as an anti-counterfeiting strategy for other kinds of products, both medical and non-medical.

The case for this new approach will be presented as follows: The basic concept and elements of the CNT technique are discussed first, followed by implementation issues. Statistics for the technique are briefly covered; these show that the technique can theoretically be fairly proficient at identifying counterfeits. Problems and attack strategies are analyzed next, along with intrinsic CNT attributes and possible countermeasures that can serve as mitigating factors. The next sections explain how the CNT technique differs from FDA anti-counterfeiting proposals, conventional serial number hashes, and standard product registration processes. The final section before the Conclusion offers other comments about the CNT technique.

The Proposed CNT technique

The “Call-In the Numeric Token” (CNT) Technique has 4 required components. These are: (1) a unique container identification number or “Bottle ID”, (2) a secret computer database of Bottle IDs maintained by the pharmaceutical manufacturer, (3) a dedicated web page and/or automated phone line(s) for customers to “call in” to check their Bottle ID(s), and (4) some degree of customer participation (even if far from universal). “Customer” here can mean individual consumers, but also wholesalers, repackagers, pharmacies, hospitals, and other companies and institutions that handle large volumes of pharmaceuticals.

Currently, most pharmaceutical containers or packaging are marked with the appropriate Lot Number and Expiration Date. The CNT technique requires that an additional identification (ID) number be applied. For simplicity of discussion, this ID number will be referred to as the “**Bottle ID**”, even though the ID number might instead be applied to the packaging, or even to a different type of drug container such as a tube, box, drum, pallet, or even a truck, depending on the application.

The “Bottle” ID can be inserted into, or printed on, the container (or packaging) during manufacture, or else added at a later date by applying an adhesive label. The Bottle ID doesn’t even have to be physically attached to the pharmaceutical container at all.

In randomly choosing a Bottle ID for each “bottle” (perhaps at the very instant of printing), a computer must obey the following rules:

Rule 1: The Bottle ID must be a unique number (no duplication) for each bottle within a given Lot. Thus, two bottles can have the same Bottle ID only if they come from a different manufacturing Lot.

Rule 2: The ID is not a serial number; it must be random, non-sequential, and unpredictable.

Rule 3: There must be at least 1000 times more possible Bottle IDs than actual bottles produced for a given Lot.

Figure 1 shows an example of the markings on a bottle under the CNT scheme. The Bottle ID format in this example (3 letters followed by 3 numeric digits) allows about 17.6 million unique ID numbers, and thus up to 17,576 different bottles (under Rule 3 above) for this Lot. See Table 1. It is not actually necessary to use a consistent format for the Bottle ID numbers, either within a given Lot or between Lots. Variability can further frustrate the counterfeiters’ task of determining valid ID numbers.

A computer needs to keep track of the actual Bottle IDs printed for a given Lot. Only those Bottle IDs are authorized or “**valid**”; a non-valid Bottle ID indicates a counterfeit product. The database of valid Bottle IDs needs to be kept secret by the pharmaceutical manufacturer, at least until the appropriate Lots expire.

Note that keeping track of the valid Bottle IDs via computer requires only modest storage. For example, a maximum of 53 kBytes are needed per Lot for the (3 letter + 3 digit) Bottle ID format shown in figure 1. (~3 bytes x 17,576 bottles.) Thus, a single CD or DVD could hold

data for 250 million and 1500 million bottles, respectively. Data compression would permit an even greater capacity.

The pharmaceutical manufacturer, the government, or an association of manufacturers, would need to establish a public Internet site and/or dedicated phone line. Ideally, the phone line is automated with voice recognition software to simplify its use for consumers. The web site and/or phone line allows customers to quickly check whether their Bottle IDs are valid for the appropriate Lot Number(s). (This is termed "**calling in**".) Customers are only given a yes/no response, i.e., they are told only that the bottle appears to be authentic or not. If the latter, they would be encouraged to return the counterfeit drugs to the manufacturer for analysis, and to obtain a replacement.

Regardless of the number of other customers who "call in", a customer's invalid Bottle ID(s) can be immediately identified by the web site or phone line with essentially 100% accuracy when she calls in. An invalid Bottle ID (unless the customer made an error or is not being sincere) is a sure indication that the drug is counterfeit.

Even without calling in, high-volume customers can spot some counterfeits by simply noting duplicate Bottle IDs within their own (current and previous) stock.

If multiple customers call in identical, valid Bottle IDs, this indicates that most or all of their pharmaceuticals are counterfeits. It tells us that the counterfeiters are replicating at least some valid Bottle IDs to assist in their drug counterfeiting. See below for a discussion of how counterfeiters can obtain valid Bottle IDs, and why it is challenging to obtain large numbers of them.

If only a few Bottle IDs are found to have been replicated in large numbers by counterfeiters, pharmaceutical manufacturers could issue public warnings about those specific Bottle IDs. The FDA's MedWatch system[6] would be one mechanism. This might alert even customers who don't call into the CNT system.

Implementation

It may be advantageous to bar-code the Lot Number and Bottle ID on the bottle or packaging, or encoded them in a radio frequency transducer (RFID) or memory contact button, or read them using computer character recognition. This would make it possible to automate the calling-in process for wholesalers, repackagers, pharmacies, hospitals, institutions, and others who possess large quantities of drugs.

The fact that bar codes, RFIDs, or contact memory buttons are relatively easy to counterfeit[12,17] makes them ineffective as anti-counterfeiting tags. Under the CNT scheme, however, being able to counterfeit these technologies is not of help to an adversary unless he knows which Bottle IDs are valid. In the CNT technique, it is the Bottle ID number itself which serves as the tag or token, not some physical device.

There are a number of other ways to record the Bottle ID in or on the pharmaceutical product. The Bottle ID can, for example, be placed inside the tamper-evident packaging; it can also be

written on scratch-off labels such as used for lotteries. This complicates the task of a counterfeiter who may want to gain access to large numbers of valid Bottle IDs without actually purchasing the pharmaceuticals. Of course, while placing the Bottle ID inside the tamper-evident packaging may be practical for individual consumers or repackagers, it creates difficulties for wholesalers who may not want to open large numbers of containers to determine Bottle IDs. On the other hand, we may want to vary the CNT approach for different customers and container types/sizes.

The Bottle ID might also be printed on a tear-off tab or removable adhesive label. That would reduce the chances of a given bottle being inadvertently called in twice by the same owner. (See Scenario 7 below.) A magnetic stripe that is erased in the process of being read can accomplish the same thing, as can a frangible film, with the Bottle ID printed on it that is destroyed when the consumer attempts to withdraw the first pill. The obvious disadvantage to these one-shot approaches is that a bottle cannot be easily checked by the new owner if it is resold.

It is important to note that the Bottle ID is a kind of “virtual” tag or token. It is not actually necessary for the Bottle ID to be physically inside or attached to the packaging, or even shipped at the same time as the drugs. This has important implications for repackagers and pharmacies. (See Scenario 9 below.) The Bottle IDs can be mailed or emailed to a customer at a later date. The Bottle ID in this situation is thus truly a “buddy” tag or token, not a physical tag. Each valid Bottle ID (and associated Lot Number) is, in effect, a kind of authorization to own 1 bottle. If the bottles are resold, the purchaser must insist on receiving an equal number of valid Bottle IDs. He should call in each of the Bottle IDs to see if they are indeed valid.

For licensed wholesalers or other authorized high-volume customers, it might be prudent to provide free software and readers. These would allow them to easily record Bottle IDs, check their stock locally for Bottle ID duplicates, and automatically call-in to be alerted to other counterfeits. The software would also help prevent the customer from inadvertently calling in a given bottle twice, thus improving the accuracy of the CNT results. If the reader and software record the Bottle IDs in an encrypted form (especially using a public/private key cipher[19]), it would be more challenging for an adversary to steal the recorded valid Bottle IDs.

Statistics

As discussed above, anyone who calls in with an <u>invalid</u> Bottle ID (assuming he did not make a mistake and that he is not deliberately trying to spoof the CNT system) will be told correctly 100% of the time that he has counterfeit drugs. This is true regardless of the number of previous or subsequent callers.

Now consider the situation where there exists in the world 1 legitimate bottle, and N counterfeit bottles, all printed with the same <u>valid</u> Bottle ID. The probability that any one of these bottles will be correctly identified as counterfeit when called in is N/(N+1). (This assumes that at least 2 of these bottles are called in, permitting the counterfeiting to be detected in the first place.) Table 1 shows that the CNT error rate is very low in identifying counterfeits when the counterfeiters make even a relatively small number of counterfeit bottles with the same valid Bottle ID.

For reasons discussed below, we may instead want to use a threshold greater than 2 callers before deciding that counterfeiting of a given Bottle ID has occurred. In general, when the number of callers (calling in the same Bottle ID) reaches some threshold value, T, we will report counterfeiting to that caller and all subsequent callers. Let C be the ultimate, final total number of callers reporting the same valid Bottle ID. Assuming we do not try to re-contact previous callers who made an inquiry prior to the threshold T being achieved, the percentage of total callers who will be told they hold counterfeits is equal to 100% x (C-T+1)/C. This is plotted in figure 2 for four different thresholds, T.

The key point in figure 2 is that even with a high threshold (e.g. T=10), we can still correctly notify a significant portion of callers that they probably have a counterfeit. Of course, once the threshold is achieved for a given Bottle ID, we could always re-contact the T-1 previous callers (assuming they have offered their identity and contact information) to warn them that new information suggests they might have counterfeit drugs after all. This would make 100% of the callers reporting the same (valid) Bottle ID aware that they probably hold a counterfeit.

Attacks, Problems, and Countermeasures

This section briefly outlines some of the problems with the CNT technique, and possible attack strategies for counterfeiters. Implications, mitigating circumstances, and countermeasures are also discussed.

Scenario 1 - Guessing Bottle IDs

Counterfeiters can randomly guess Bottle IDs. Their problem, however, is that the odds of guessing a valid Bottle ID (for a given Lot Number) are less than 1 in 1000 because of Rule 3 above. As a result, fewer than 0.1% of their counterfeit bottles (on average) will pass the call-in test. Even without calling in, high-volume customers may be able to spot the counterfeits by detecting replicate Bottle IDs within their own stock.

Scenario 2 - Phishing for Bottle IDs

Counterfeiters can always try to “phish” for valid Bottle IDs by calling in trial numbers. On average, however, it will take at least 1000 tries to get a valid Bottle ID. We can virtually eliminate this attack scenario if the callers are only given a Yes/No decision on their Bottle ID (and not allowed access to the whole database), and if we disallow unlimited inquiries from a single, unknown caller if he inquires about a large number of invalid Bottle IDs. Requiring some form of identification (such as a password, drug business license, prescription number, or invoice number) for callers may make sense for a number of reasons, especially for customers claiming to hold a large amount of stock.

Scenario 3 - Other Ways to Obtain Valid Bottle IDs

Another approach that drug counterfeiters can use to obtain valid Bottle IDs is to buy some of the authentic product. They might also try to quickly examine large supplies of the product (without purchasing) in order to record valid Bottle IDs. As a practical matter, it is likely to be time consuming, expensive, risky, and/or difficult to obtain large numbers of valid Bottle IDs. (This is especially the case if the Bottle IDs are placed inside the tamper-evident packaging.)

They may be more inclined to make duplicate Bottle IDs from a relatively small number of valid numbers. But these can be detected by CNT call-ins.

Valid Bottle IDs can be obtained by one or more of the following methods:

- Legitimate products are purchased, the Bottle IDs extracted, and then the products are discarded. This can be expensive for the counterfeiters.

- Legitimate products are purchased, the Bottle IDs extracted, and then the products are resold. Returning the authentic product to the marketplace may increase the chances that the counterfeiter can be traced.

- Nefarious insiders gain access to the secret Bottle ID database kept by the pharmaceutical manufacturer. Good security, however, can minimize this possibility. Furthermore, the Bottle IDs stored in the database are of no value once the Lots expire, or for future pharmaceuticals not yet manufactured or packaged.

- Nefarious insiders gain access to significant numbers of valid Bottle IDs at high-volume handlers, or while pharmaceuticals are in transit. Good security can help minimize this risk.

- Counterfeiters record valid Bottle IDs at retail stores or pharmacies. This may be difficult to do in large numbers, especially if the Bottle IDs are placed inside the tamper-evident packaging.

Scenario 4 - Denial of Service Attacks

Counterfeiters (or hackers) can try to sabotage the CNT system by Denial of Service (DoS) attacks.[10] This involves tying up the call-in web site and phone lines with nuisance contacts. Counterfeiters do not benefit directly from such actions, but they might discredit the CNT system and impede or upset customers.

DoS attacks can be at least partially mitigated by using standard DoS countermeasures,[10,18] by requiring callers to identify themselves, and/or by setting up private web sites and phone lines (unavailable to the public) for trusted, high-volume customers.

Scenario 5 - Spoofing the System

Counterfeiters (or hackers) could try to sabotage the CNT system by calling in valid Bottle IDs multiple times. Those Bottle IDs would then be incorrectly identified as having been counterfeited. Such spoofing is of no value unless they possess significant numbers of valid Bottle IDs—which is non-trivial as discussed previously.

This attack can be partially mitigated by raising the threshold, T, to a larger value than 2. As shown in figure 2, this only slightly reduces the efficiency of the CNT technique. Another countermeasure is to establish secret or private web pages and phone lines for use only by trusted wholesalers, pharmacies, and hospitals. Also, requiring callers to identify themselves (such as via a password) can be useful, as can building in delays in the CNT system for individual consumers, making calling in large numbers of valid Button IDs very time consuming.

While they might discredit the CNT system and upset customers, the counterfeiters (or hackers) do not benefit directly from spoofing the CNT system in this manner. Moreover, the attacks may backfire. Creating the appearance of extra drug counterfeiting could focus more worldwide attention on the drug counterfeiting problem. This might encourage governments or pharmaceutical manufacturers to take additional anti-counterfeiting measures and increase prosecution—something not in the best long-term interests of the counterfeiters.

Scenario 6 - Fake Call-In Sites

Counterfeiters can establish fake web sites and phone numbers that incorrectly tell callers that their pharmaceuticals are authentic, even when this is not the case. The counterfeiters might print their fake Internet URL and phone number on the counterfeit bottles, or placed them inside the counterfeit packaging.

Pharmaceutical manufacturers can counter this attack by not including the URL or phone number for CNT call-ins on (or inside) the legitimate product. Instead, customers and consumers would need to be educated as to the correct URL or phone number to use. This could be accomplished by an extensive national or worldwide advertising campaign, including listings in telephone books, memorable radio and television jingles, and the use of a URL and phone number (e.g., 555-FAKE) that can be easily remembered. Manufacturers might also want to periodically contact major customers directly to make sure they have the correct URL and phone number. Providing free inventory and call-in software to high-volume customers might help prevent the use of bogus URLs and phone numbers.

Pharmaceutical manufacturers might want to use company sales representatives to provide physicians and pharmacies with informational handouts for their patients. These would contain the correct URL and phone number, as well as call-in instructions. (The assumption here, of course, is that the physicians and pharmacies will actually pass along the correct information, instead of replacing it with false information if they are serving as the counterfeiters.)

It might also be prudent to continually scan the Internet to detect counterfeit call-in sites.

Scenario 7 - Innocent Redundancy by Customers

Consumers or other customers might innocently call-in the same bottle more than once. This can skew the counterfeit detection. Countermeasures to this problem include setting the threshold above 2; using tear-off, scratch-off, or frangible printing for the Bottle ID to minimize reuse; understanding the identity of the callers; and/or providing high-volume customers with software that prevents this kind of error.

Scenario 8 - Duplicate Calls Due to Drug Resale

Pharmaceuticals are often resold by the original purchaser. (The FDA, however, has proposed that limiting the number of legal drug resales might be an effective anti-counterfeiting measure.[6]) Drug resales could lead to duplicate CNT call-ins for the same bottle if both the original and subsequent owners call in.

There are several possible ways to deal with this issue. If the seller is a repackager, see the next Scenario. Otherwise, the threshold could be increased beyond 2. The use of tear-off tabs for the printed Bottle ID would cause the Bottle ID to be missing for the second owner—

eliminating the duplication problem, but also offering no chance for the new owner to check on authenticity. The reseller could instead report to the pharmaceutical manufacturer which Bottle IDs were sold, though this requires extra work.

If both the original and new owners call-in and identify themselves, we can check to see if the sale is going in the correct direction, e.g., not from consumer to wholesaler, or consumer to consumer. Another approach would be to limit the CNT system to use only by one class of customers: licensed wholesalers only, pharmacies only, or consumers only. Then reselling would be less of an issue, though the efficiency in detecting counterfeits would decrease. Separate and unconnected CNT systems could also be run for each class of customers.

Scenario 9 - The Repackaging Problem

Unit of use (single dose) packaging, of course, would eliminate many of the problems associated with repackaging. The question of how to otherwise handle repackaging is a critical one. According to the FDA, "Repackaging destroys anti-counterfeiting technologies employed by the manufacturer."[6] With CNT, however, putting the Bottle ID inside tamper-evident packaging is not necessarily a problem for repackagers or pharmacies. They must typically open the packaging, anyway.

Repackagers can use the fact that the Bottle ID is a virtual tag, not necessarily a physical one. Thus, under CNT, a Bottle ID can be reused by repackaging, re-adhering, or reprinting it. If the repackager is consolidating small "bottles" into larger ones, he needs to only reuse a subset of the original Bottle IDs. He should then destroy the unused Bottle IDs; they become a vulnerability if stolen by (or sold to) counterfeiters, or if the repackager himself is a counterfeiter.

How do we handle the more common situation where a repackager or pharmacy is "sub-dividing", i.e., creating more new "bottles" than the number of old bottles? There are several possibilities. Repackagers might be required to obtain authorization from the pharmaceutical manufacturer (or be sent new printed labels) for imprinting new Bottle IDs. Alternatively, they might be able to simply contact the manufacturer to state that some of the Bottle IDs will be re-used. The manufacturer can factor this information into the CNT call-in system and the choice of threshold.

A third and probably more practical approach is for the pharmaceutical manufacturer to automatically pack (a reasonable number of) multiple Bottle IDs—each one different—inside a single large bottle. (This could be done in the form of removable adhesive labels, though there are other possibilities.) Each new bottle created by an authorized repackager or pharmacy would then get one of these unique Bottle IDs that came with the original big container. This approach represents an extension of Rule 1 above, where we now create a unique Bottle ID for each virtual or future bottle. The Bottle IDs represent a kind of authorization to create a fixed number of new bottles. Unused Bottle IDs represent a vulnerability if made available to counterfeiters.

Fortunately, each unused Bottle ID that a repackager or pharmacy allows to fall into the hands of counterfeiters represents only one counterfeit bottle that the counterfeiters can safely make. If they replicate the diverted Bottle ID multiple times, the CNT call-in system has the possibility of detecting the counterfeits. Moreover, some traceability of the bootlegged Bottle

IDs—pointing back to the guilty repackager or pharmacy—may be possible if CNT callers identify themselves.

Scenario 10 - Identity & Privacy Issues

Though not required, having callers identify themselves can greatly improve the security and effectiveness of the CNT technique. (For example, earlier callers can be re-contacted when it appears that a given Bottle ID has been counterfeited based on the call-in threshold. Also, instances of counterfeiting that are discovered may become traceable if the callers are known.) Having callers identify themselves, however, may raise privacy concerns and possibly discourage consumers from participating. Moreover, having to type in a password or identity information during the call-in will slow down what would otherwise be a very rapid yes/no response on the Internet or telephone.

Scenario 11 - The Best as the Enemy of the Good

The CNT technique is only a partial solution to product counterfeiting. It makes no *a priori* attempt to stop the counterfeiting, nor will it detect all counterfeits. Sometimes implementing partial measures to deal with hazards puts manufacturers in a risky situation in regards to liability. The way to counter this problem is to involve the government and/or make the CNT approach—even if imperfect—an industry best practice. Due diligence could then be claimed even if the counterfeiting problem is not totally eliminated.

A more specific problem is how to deal with a caller who is told his drugs are likely to be counterfeit when they really aren't. Ignoring caller error, this can occur when a valid Bottle ID is replicated by counterfeiters N times. One (but only one) customer will possess the single authentic bottle with that Bottle ID. If he calls in, we cannot distinguish his sole authentic bottle from the N fakes. If his drugs are mailed in for analysis, however, we can notify him later of the error, along with an apology and a statement that this was all in the interest of his safety and the greater good.

How Does CNT Differ from FDA Proposals?

In its 2004 report, "Combating Counterfeit Drugs"[6] the FDA calls for "mass serialization" of pharmaceutical containers and extensive use of RFIDs for purposes of tracking "pedigree". CNT differs from this approach as follows:

1. The CNT Bottle ID is not a serial number because it is random, unpredictable, and non-sequential.

2. The CNT Bottle ID, unlike the FDA's "serialization code", does not contain information about the product that can be used to help guess valid numbers. Indeed, the CNT Bottle ID requires far fewer bytes (2-4) than the 12-byte minimum code envisioned by the FDA.[6]

3. The CNT technique does not attempt to track or trace drug pedigree; this is not necessary under CNT to detect counterfeits. (Data from CNT callers might nevertheless be useful for tracing pharmaceuticals, particularly if customer participation is relatively high and/or if callers identify themselves.) Even with high-technology, tracking or tracing pharmaceuticals like the FDA envisions will be a daunting task.

4. Unlike CNT, the FDA approach does not involve voluntary customer call-ins, and would not directly involve consumers. Tracking throughout the logistics chain won't help if counterfeiters slip consumers fakes at the point of final delivery, and they have no way to check authenticity.

5. Unlike the system envisioned by the FDA, counterfeiting RFIDs (or other high-tech tags) is not a relevant attack on the CNT technique. This is because the Bottle ID is a token or virtual tag; its security and functionality does not depend on the specific mechanism used to record or encode it on the container or packaging.

How Does CNT Differ from a Hash Based on Serial Numbers?

Another, non-tag approach to checking authenticity of a product is to compute a hash from the product's model and serial number, then encode the hash with a public/private key. (A "hash" is a fixed-length number--something like a checksum or parity check--computed from other letters and numbers.[19]) Customers can computationally decrypt the hash to see if it valid (because they possess the public key), but cannot easily encrypt a different hash to make a counterfeit (because they lack the private key).[19]

The major problem with the hash approach for anti-counterfeiting purposes is that a counterfeiter needs to merely buy or examine one legitimate product, then produce multiple counterfeits with exactly the same model number, serial number, and hash. Purchasers of the counterfeit product will be unaware they bought fakes because the hash will decrypt properly.

The call-in feature of the CNT technique discussed in this paper is what permits duplicate counterfeits to be detected. The Bottle ID in the CNT scheme plays the role of a hash, but is randomly assigned, rather than being computed like a conventional hash.

To summarize the differences between the CNT technique and a hash method:

1. The CNT Bottle ID is not a serial number because it is random, unpredictable, and non-sequential.

2. Duplicate serial numbers and hashes are not detected by the hash approach because there is no customer call-in. While counterfeiters can't compute the encrypted hash for a given serial number, they can infinitely copy a single serial number and hash without customers or the pharmaceutical manufacturer easily finding out.

3. The hash technique is computationally intensive (especially for public/private keyed hashes) and requires complex key distribution methods.[19] This is not the case for the CNT method.

4. With the CNT technique, customers who call-in can benefit other customers and the pharmaceutical manufacturer, as well as themselves. There is no equivalent for the hash method.

5. Nefarious insiders within the pharmaceutical manufacturer who can gain access to the private hash key will be able to compute future hashes. This is a potential security vulnerability. With the CNT technique, however, even insiders with access to the secret database cannot predict future Bottle IDs because they have not yet been assigned.

How Does CNT Differ From Standard Product Registration?

Manufacturers of consumer products often request that customers register the serial number of their purchase on the Internet, or by mailing in a postcard. A good example of this practice is the software industry.

The differences between the CNT technique and software registration include:

1. In principle, registering the software license or registration key could be used by software companies to monitor software counterfeiting. In practice, however, the registration process is primarily for the purpose of gathering marketing information and being able to inform customers of future upgrades.

2. As such, customers gain little benefit from the registration process, unless it is required to make their software work. The point of the call-in process in CNT, in contrast, is to directly benefit the customer by verifying the authenticity of his purchase. Moreover, under CNT, callers benefit from the call-ins of other callers. Even non-callers can potentially benefit if widespread counterfeiting is detected and the pharmaceutical manufacturer issues a notification to the public via the news media or MedWatch.

3. There is usually no equivalent of Lot Number or Expiration Date with software.

4. With software, the counterfeit product is often functionally identical to the authentic product because it is an exact copy. There is thus little incentive for most customers to worry about counterfeiting. This is not usually the case with counterfeit drugs.

5. Purchasers of software are often automatically connected to the registration web site when their software is first installed. Alternately, they may be encouraged to mail-in a post card that is included with the product. This is not a secure practice because counterfeiters could easily direct the customer to a bogus web site or mailing address. With the CNT technique, in contrast, there must be an independent way for customers to know the correct call-in URL or phone number. This information cannot be printed on, or included with the pharmaceuticals because there is no easy way to guarantee its authenticity.

6. With software, customers who buy many copies of a given program are usually issued a single license number, with no unique identifier for individual copies of the program. This is not the case for pharmaceuticals and the CNT method.

7. The registration key for software is sometimes a kind of hash of the customer's name and organization. A nefarious insider within the manufacturer may be able to generate valid, unauthorized registration numbers for future use if he can access the hash function. With CNT, in contrast, nobody can calculate valid Bottle IDs because they haven't been picked yet. Moreover, the hash used for some software licenses isn't necessarily secure. A sophisticated adversary might be able to figure out the hash algorithm by studying multiple copies of the software.

8. The registration or license number typically stays with the software program, whereas one option for CNT is tear-off or destructible Bottle IDs.

9. Software registration requires the customer to identify himself. This is only an option for CNT.

10. Software registration keys are often much longer than the Bottle IDs needed for CNT, often 16 or more bytes vs. 3-5 for CNT.

Additional Comments

Alternate Means of Calling In

Consumers might find it particularly easy to hold the bottle up to the phone, press a button on a microchip, and let the bottle "beep" its Lot Number and Bottle ID into the phone using standard telephone touch tone frequencies.[20] Currently, micro-circuits on greeting cards can talk or sing; these cost under $2 each in quantity (including the battery), and prices are certain to decrease over time.

CNT Costs

Nowadays, the cost for automated printing of individual numbers on the fly (even randomly chosen numbers) onto containers or adhesive labels is very low. Costs are also modest for maintaining a single automated CNT database, which could be implemented on a single personal computer. The costs of establishing and running a CNT web site should also be modest because the web site is little more than a big look up table. Having a bank of automated, voice-recognition phone lines for CNT callers, on the other hand, would be more expensive. Probably the greatest cost associated with CNT would be in educating customers and the public, including consumers, pharmacists, and physicians about the CNT system and which URL or phone number to use.

Initially, the use of a CNT system might be limited to high-volume customers only. Pharmaceutical companies might also keep costs down by establishing a joint CNT system with other manufacturers, or by seeking government sponsorship.

It might also make sense not to routinely recommend that customers call in unless/until there is an independent evidence for widespread counterfeiting of a particular drug, and/or there is a public counterfeit scare that requires positive action.

CNT as a Service

If the Bottle IDs are printed in advance as adhesive labels or inserts, the entire CNT system could be run by a third party as a relatively small service business. Bottle IDs would be (securely) provided to pharmaceutical manufacturers as needed. Responsibility for maintaining the CNT database and operating the web site and phone lines would rest with the service provider.

Additional Benefits

Asking customers—especially consumers—to take personal responsibility for checking the authenticity of their own medicines may have significant educational, behavioral, legal, and public health benefits. Fortunately, customers who aren't concerned about counterfeiting will not be bothered; they can just ignore the CNT system.

For pharmaceutical companies, Information provided by CNT callers can lead to a better understanding of customers and the market. Pharmaceutical companies might also benefit from enhanced public and government good will by taking proactive measures to deal with counterfeiting. Moreover, if CNT callers can be encouraged to mail in their counterfeit pharmaceuticals, we stand to learn more about the nature and extent of counterfeiting, and perhaps can more rapidly identify public health risks.

Conclusion

The “Call-in the Numeric Token” (CNT) technique is based on the idea of assigning a unique, unpredictable ID number (i.e., a virtual tag or token) to each pharmaceutical container made by a manufacturer. Customers are then encouraged to use a web site or phone line to check on the validity of the numeric (“virtual”) tag found on or in the pharmaceutical container(s) they possess. Invalid numeric tags can be spotted immediately. Furthermore, the pooling of information from callers helps to spot (and perhaps trace) ID numbers that have been illegally replicated by counterfeiters. Counterfeiters are hampered by the fact that guessing valid ID numbers isn’t practical, replicating valid IDs may be detected by the call-in process, and obtaining large numbers of valid ones will be challenging.

The CNT technique—while certainly not a silver bullet for stopping all counterfeiting of pharmaceuticals—does appear to offer (at least in principle) the potential for impeding counterfeiters at relatively modest cost. It does not require expensive, high-tech devices that are vulnerable to simple attacks. Mostly familiar technologies like the Internet and the telephone are involved. In the absence of practical, effective anti-counterfeiting tags, CNT—in its various possible flavors—may be worth considering.

Acknowledgments & Disclaimer

Anthony Garcia, Eddie Bitzer, Otis Peterson, Jon Warner, and Alicia Herrera offered useful suggestions and assistance. This work was performed under the auspices of the United States Department of Energy (DOE). The views expressed in this paper are those of the author, and should not necessarily be ascribed to Los Alamos National Laboratory or DOE.

References

1. Wertheimer AI, Chaney NM, and Santella T. Counterfeit pharmaceuticals: current status and future projections. J Am Pharm Assoc (Wash DC) 2003 Nov-Dec; 43 (6): 710-7

2. Rudolf PM and Berstein, BG. Counterfeit drugs. New England Journal of Medicine 2004 April 1; 350 (14): 1384-6

3. World Health Organization. Substandard and counterfeit medicines. Available from URL: http://www.who.int/mediacentre/factsheets/2003/fs275/en [Accessed 2004 October 25]

4. World Health Organization. Essential drugs and medicines policies. Available from URL: http://www.who.int/medicines/organization/qsm/activities/quality assurance/cft/CounterfeitOverview.htm [Accessed 2004 October 25]

5. Hopkins DM, Kontnik LT, and Turnage MT. Counterfeiting exposed: how to protect your brand and market share. New York: Wiley, 2003

6. United States Food and Drug Administration (FDA). Combating counterfeit drugs. 2004 February. Available from URL: http://www.fda.gov/oc/initiatives/ counterfeit/report02_04.html [Accessed 2004 October 15]

7. Johnston, RG. Tamper detection for safeguards and treaty monitoring: fantasies, realities, and potentials. Nonproliferation Review 2001 Spring; 8 (1): 102-115

8. Johnston RG and Garcia ARE. An annotated taxonomy of tag and seal vulnerabilities. Journal of Nuclear Materials Management 2000 Spring; 229 (3): 23-30

9. Johnston, RG. Tamper-indicating seals for nuclear disarmament and hazardous waste management. Science and Global Security 2001; 9 (2): 93-112

10. Anderson RJ. Security engineering. New York: Wiley, 2001

11. Los Alamos National Laboratory. Vulnerability assessment team home page. Available from URL: http://pearl1.lanl.gov/seals.default.htm [Accessed 2004 October 20]

12. Johnston RG, Garcia ARE, and Pacheco AN. Efficacy of tamper-indicating devices. Journal of Homeland Security 2002, April 16. Available from URL: http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50 [Accessed 2004 August 12]

13. Johnston RG and Garcia ARE. Analyzing vulnerability results for tags and tamper-indicating seals. Proceedings of the U.S. Army Conference on Applied Statistics; 2001 October 24-26; Santa Fe, NM. pp. 60-88

14. Karsten R. Tags tag counterfeits: as counterfeiting methods become increasingly sophisticated, more advanced technologies are needed to fight back. Manufacturing Chemist 2003 January 1; 73 (1): pp-p

15. Deisingh A. Counterfeit drugs. Chemistry and Industry 2004 March 15; 54 (6): 16-18

16. Kontnik, L. Counterfeits: the cost of combat. Pharmaceutical Executive 2003 November 1. Available from URL: http://www.pharmexec.com/pharmexec/article/articleDetail.jsp?id=75674 [Accessed 2004 November 5]

17. Johnston, RG. The state of the art—an introduction to technology. Proceedings of the National Cargo Security Council Conference on Security Technology; 2004 July 18-20; Linthicum Heights, MD

18. Mirkovic J, Dietrich S, Dittrich D, et al. Internet denial of service: attack and defense mechanisms. New York: Prentice Hall, 2004

19. Menezes AJ, van Oorshot PC, Vanstone SA. Handbook of applied cryptography. New York: CRC Press, 1997

20. Elert, Glenn. Beats. The Physics Handbook: Beats. Available from URL: http://hypertextbook.com/physics/waves/beats/ [Accessed 2004 November 5]

Table 1 - The number of unique Bottle IDs and bottles allowed per Lot for various Bottle ID formats. To avoid confusing letters with numeric digits, the letters O and I (and letter L if lower case letters are used) might be excluded—somewhat reducing the values in columns 2 and 3.

bottle ID format	no. of unique IDs	maximum no. of bottles per lot
6 digits (2.5 bytes)	1 million	1,000
7 digits (2.9 bytes)	10 million	10,000
3 letters + 3 digits (3.0 bytes)	17.6 million	17,576
4 letters + 3 digits (3.6 bytes)	457 million	456,976

Table 1

Table 2 - Accuracy in telling the next caller that he has a counterfeit under the assumption that the same valid Bottle ID has already been called in multiple times, and that there exists 1 authentic bottle, and N counterfeit bottles, all with the same valid Bottle ID. This table shows that by the time counterfeiters have made more than just a few replicates of the same Bottle ID, we can have great confidence that any one of the bottles called in with that ID is a counterfeit.

no. of counterfeits made (N)	accuracy= N/(N+1)	error rate
2	67%	33%
10	91%	9%
100	99%	1%
1,000	99.9%	0.1%
10,000	99.99%	0.01%

Table 2

Lot: 4ZB1026
Exp: 04/06
Bottle ID: KSD709

Figure 1 - An example of the printing applied to a pill bottle, packaging, or other pharmaceutical container under the CNT scheme. In this case, the Bottle ID consists of 3 letters (A-Z) and 3 numeric digits (0-9).

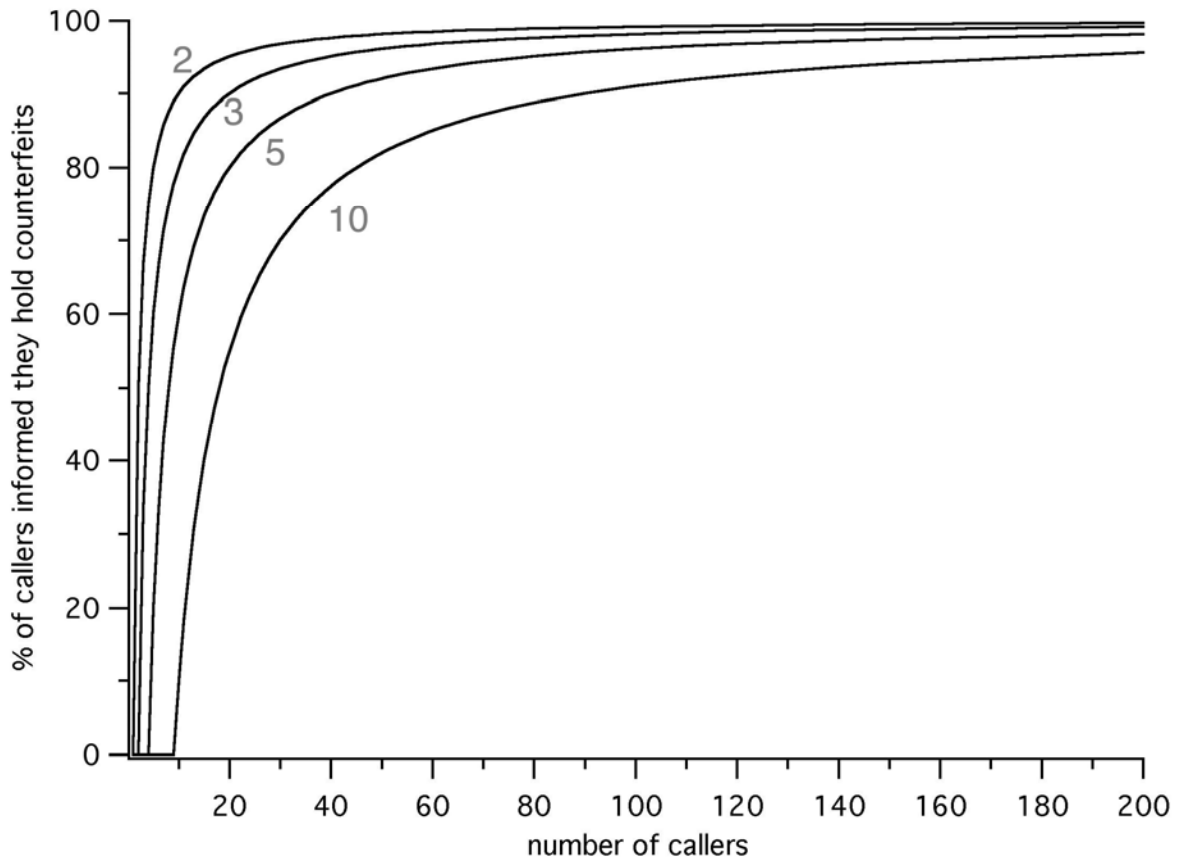

Figure 2 - Percentage of callers reporting the same (valid) Bottle ID who will be notified their drugs are counterfeit vs. the number of callers reporting that Bottle ID. This is plotted for 4 different thresholds (2, 3, 5, and 10 callers). The assumption for this graph is that counterfeiters have created a large number of counterfeits with the same (valid) Bottle ID number. Note that if earlier callers are re-contacted after the call-in threshold has been achieved for a given Bottle ID, then 100% of all callers will be informed they hold counterfeits rather than the percentage plotted here.