Overview of the Selection of Strategic Authentication and Tracing Programmes

John Spink

9.1 Introduction

There is a wide range of pharmaceutical product threats, including counterfeit and substandard products. Consumer products, including pharmaceuticals, must be protected from fraudsters and criminals (the term 'fraudster' is used as a descriptive, formal term for this specific type of criminal and their activity [1–3]). The goal is not to see how many infringers can be caught: the goal is to reduce the prevalence of counterfeit product in the first place – to reduce the vulnerability and determine which countermeasures also increase our probability of finding new or evolving threats. To be most efficient and effective, the countermeasures must be strategic, holistic, interdisciplinary, all-encompassing and proactive rather than single-discipline, narrow, reactive and tactical.

This chapter is based on experience and expertise gained through engagements and research projects with industry brand owners and security suppliers, government enforcement and prosecution agencies, as well as a wide range of associations and academic thought leaders. The approach is extremely interdisciplinary and grounded in the behavioural sciences and criminology with a focus on reducing fraud opportunity in the first place.

Anti-counterfeit strategy is within the broader 'brand protection' concept, which is under the even broader concept of 'product protection'. Product protection includes a wide range of concepts that focus on consumer or patient safety. The broader concepts often include: tamper resistance, child resistance, universal design/senior-friendly, cargo theft, shoplifting, return fraud, warranty fraud, expiration date monitoring and management, and support of more effective recalls.

Counterfeit Medicines Volume I: Policy, Economics and Countermeasures, edited by Albert I. Wertheimer and Perry G. Wang.

Picking a single technological solution and hoping it is a magic solution is easy, but technology is only one of the many aspects of an anti-counterfeit strategy. The solutions are systems, not tools, and must include what is referred to as a layered-approach. What is difficult is strategically explaining why and how it will help – including in comparison with *all* other countermeasures – and to not only expect but also anticipate how the bad guys will try to circumvent this system or countermeasure. The term 'bad guys' is often used in practice and is used here to focus attention on situations where there is clear agreement that actions are criminal, fraudulent and an infringement. Many criminal or fraud initiatives get sidetracked by divergent definitions of the criminal nature of diversion, compulsory licensing and intellectual property rights. Using the term 'bad guys' also helps to define collaboration by the 'good guys'.

This chapter provides a framework to review the problem and solutions, the nature of fraud and fraudsters and how countermeasures detect and deter bad guys. It also includes a review of current countermeasures.

9.2 Anti-counterfeit Strategy: Overview

Anti-counterfeit strategy considers holistic, all-encompassing, proactive solutions rather than a single-discipline, narrow, reactive, tactical countermeasure. Anti-counterfeit strategy is about bad guys not bad medicine. Understanding anti-counterfeit strategy is based on understanding the nature of the fraud and the fraudster [4]. When this is achieved, there is a better chance of not only combating current risks but, by understanding the inherent vulnerability, predicting and anticipating the next moves as well. According to Spink and Moyer [5], the counterfeit and substandard medicines 'public health threat is similar to a disease that requires continual surveillance, monitoring and treatment (e.g. diabetic populations) rather than treating a single event (e.g. a broken bone)'. As companies and countries are facing a more complex and risky counterfeiting threat, there has been a shift from tactical (reactive) to strategic (proactive) countermeasures. Anti-counterfeit strategy should be considered a chess match with the intelligent adversaries.

There are three key end-of-supply chain participants. For this chapter:

(a) a *consumer* is the last person receiving the benefit of the product – this might not be the person that purchased the product
(b) the *customer* is the person who made the purchasing decision
(c) the final customer group is the *user* who would apply the product for the consumer.

9.2.1 Types of Counterfeiters and Counterfeiting

Criminals have been studied in the criminology or criminal justice fields for years. Select types of criminals that most readily apply to counterfeiting are included in Table 9.1 [6, 7]. More generally, these are types of fraud since, in some countries or with some products, some of the activities are not defined as criminal or even a civil

Table 9.1 Criminal types and attributes applicable to food fraud [6]. (Source: Adapted from Hagan, F. (2010). *Crime Types and Criminals*. Sage Publications, Thousand Oaks, CA.)

Type of criminal	Definition
Recreational	Acts for entertainment or amusement
Occasional	Acts infrequently or opportunistically
Occupational	Acts at their place of employment, either as an individual or with the company's knowledge
Professional	Crime fully finances their lifestyle
Ideological	Domestic or international terrorist who commits acts to make an ideological statement or to economically harm an entity

law violation – some actions may be deceptive but are not necessarily considered unethical in some cultures.

Before discussing types of counterfeiting, it is important to note what the Organisation for Economic Co-operation and Development (OECD) refers to as 'deceptive and non-deceptive products' [8]. *Deceptive products* are products that are placed into supply chains with the intent to deceive the consumer into believing that the product is genuine in every way. *Non-deceptive* products are products that do not try to deceive the consumer into believing the products are genuine by their positioning in the market, whether through the type of retail outlet in which they are sold (flea markets, etc.), their price (exponentially low) or quality (poor) [9].

To better understand the fraud opportunity, the types of counterfeiters (Table 9.1) should be considered with the types of counterfeiting or the type of fraud (see Table 9.2 [10]). The list in Table 9.2 stretches the traditional definitions of intellectual property rights violations or even of property theft. In each case, some component or statement is fraudulent. For example, a stolen product is fraudulent when re-introduced into the supply chain unless the seller admits it is stolen – if they admit it is stolen it is still a crime. Each case represents public health vulnerability for a consumer and some benefit for the fraudster. For example, stolen goods may have spoiled due to mishandling. Counterfeiters also use stolen goods to 'salt' the market – that is, they satisfy a suspicious customer by first providing a genuine stolen product before replenishing orders with counterfeit products.

Furthermore, the types of fraudsters and types of frauds may operate in a bigger network. According to Spink and Moyer [10]:

> *The mention of the term 'organised crime' readily conjures images of hierarchical organisations such as La Cosa Nostra, Mafia, Russian mobs, Chinese Triads, or South American drug cartels. There are legal and technical differences between organised crime and criminals that are organised. Since the opportunity exists for a small fraud*

Table 9.2 Counterfeiting or fraud incident types [10]. In each case, fraudsters may not be following good manufacturing practices.

Term	Definition	Example	Potential public health threat that may lead to illness or death
Adulteration	A component of the finished product is fraudulent	Contamination of heparin	Fraudulent component
Tampering	Legitimate product and packaging are used in a fraudulent way	Changed expiry information, product up-labelling, etc.	Fraudulent packaging information
Over-run	Legitimate product made in excess of production agreements	Under-reporting of production	Fraudulent product distributed outside of regulated or controlled supply chain
Theft	Legitimate product is stolen and passed off as legitimately procured	Stolen products co-mingled with legitimate products	Fraudulent product distributed outside of regulated or controlled supply chain
Diversion	Sale or distribution of legitimate products outside of intended markets; also referred to as parallel trade, grey market or product arbitrage	Relief product redirected to markets where aid is not required	Shortages or delays of relief product to needy populations
Simulation	Illegitimate product designed to look like but not exactly copy the legitimate product	'Knock-offs' of popular products not produced with the same product safety assurances	Fraudulent product of lesser quality
Counterfeiting	All aspects of the fraudulent product and packaging fully replicated	Copies of popular product not produced with same quality and safety assurances	Fraudulent product

event to be distributed across a wide population, less sophisticated criminals who are organised cannot be ignored. Criminals form a network to perpetrate a crime, disband when the action is completed, returning to their normal, sometimes legitimate, operations and then re-form into a new criminal network, with the intent and capability of perpetrating a new fraud. Unlike traditional organised crime, these are often swarms or

networks. Disrupting any single link in the chain will not necessarily cripple the network or the ability for new fraudsters to reconnect.

The ingenuity, motivation, resources and capabilities of counterfeiters should not be underestimated.

9.2.2 Threat

The threat of product counterfeiting is on a continuum from public health to purely economic. The priority – from citizens and legislature to government agencies, enforcement and prosecution – is public health risks, then organised crime groups (including terrorism), then large economic impacts. Different products have different levels of risk. Products that are ingested, injected or implanted pose particular risks; these also include products that are procured to solve very specific problems, such as painkillers used in surgery.

Even though this chapter and section has focused on product counterfeiting and intellectual property rights infringement, it is important to emphasise that the bad guys are focused on making profit. If there were easier, less risky and more profitable options, they would pursue them. The bad guys are not focused only on intellectual property rights infringement.

9.3 Anti-counterfeit Strategy: Assessing the Situation

This section provides an overview of anti-counterfeit strategy to assist in risk assessment before choosing countermeasures. The first step is to conduct a risk assessment of the counterfeit product risk, which includes reviewing company and industry incidents. The second step is to seek to understand the nature of the fraud and fraudster, which includes understanding the criminology aspects of deterrence.

Referring to the International Standards Organization (ISO) Draft International Standard (DIS) 12931: Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods [11], counterfeiting of material goods, or physical product, is ‘to simulate, reproduce or modify a material good or its packaging without authorization’. ISO/DIS 12931 also defines a counterfeit good as a ‘material good imitating or copying an authentic material good which may be covered by the protection of one or more registered or confidential intellectual property rights’.

9.3.1 Assessment

Counterfeiters can attack at literally any and every point in the supply chain. A key concept addressed at the United States Food and Drug Administration (US FDA) February 2011 meeting was protecting the supply chain so as to control ‘participant verification’. Rogue participants are not always autonomous and completely external to the supply chain, and can range from organisations outside the supply chain, to companies in the legitimate supply chain that occasionally perpetrate fraud, to a single

individual acting alone from within the supply chain. There are numerous examples of single employees taking out genuine products (e.g. controlled substances such as oxycodone or the brand-name drug OxyContin [12]) and rogue licensed participants (e.g. a pharmacist who dilutes high-priced cancer drugs).

The demarcation between the good guys and bad guys is often blurred. ISO/DIS 12931 [11] specifically defines internal and external attacks, with the definition based on the relationship with or without the 'legitimate manufacturer, originator of the good or rights holder (staff of the rights holder, subcontractor, supplier. . .)'. In fact, 'many of the counterfeiters straddle the line between legitimate and illegitimate operations, as the opportunity presents itself' [4]. There is evidence of extensive organised crime involvement in all types of counterfeiting.

It is important to understand that, in the worst case, the counterfeiters are criminals not concerned with breaking the law, sociopaths not concerned with cheating others and not educated about the inherent public health or safety dangers. They are often '"irresponsible defendants" who flee, obfuscate ownership of their assets and effectively launder their money out of reach, who have networks that can re-form unnoticed, and who are often part of violent, criminal networks' [4].

To select optimal countermeasures, the first step is to focus on detecting or deterring the risk or vulnerability: 'to *detect* is to have methods to identify counterfeit products, with many inspection points from manufacturing to end consumer use' and 'to *deter* is to disrupt "the chemistry of the crime," or to reduce the perceived opportunity by the criminal' [13]. For every countermeasure, there should be a precise description of exactly how it detects or deters specific types of fraud and fraudsters. Many countermeasures support both functions.

9.3.2 The Fraud Opportunity

A very effective method to assess underlying fraud opportunity – and to test whether we are 'disrupting the chemistry of the crime' – is the crime triangle (Figure 9.1). This is based on well researched and widely accepted scholarly concepts.

As shown in Figure 9.1 [14, 15], the three elements of the crime triangle are the victim, the criminal (or fraudster) and the absence of a capable guardian (or hurdle). The area within the triangle represents the fraud opportunity – the bigger the triangle the bigger the opportunity. The *victim* could be a consumer receiving a fake product, a business losing a sale or a government losing tax revenue. The *fraudster* is the entity that commits the fraudulent act (the term criminal is not used since, as mentioned earlier, in some cases or countries the act may not be a crime or even a civil law violation). The *guardian or hurdle gap* is the element that monitors or protects the product. It is important to state that there is not an absence of a capable guardian or hurdle, just that if a fraud opportunity exists, fraudsters will evolve and adapt to current countermeasures and exploit new gaps.

The crime triangle is used to deconstruct the fraud opportunity and then to explain how specific countermeasures detect and/or deter specific types of fraud and fraudsters. It can be used to evaluate how authentication and traceability countermeasures reduce the fraud opportunity.

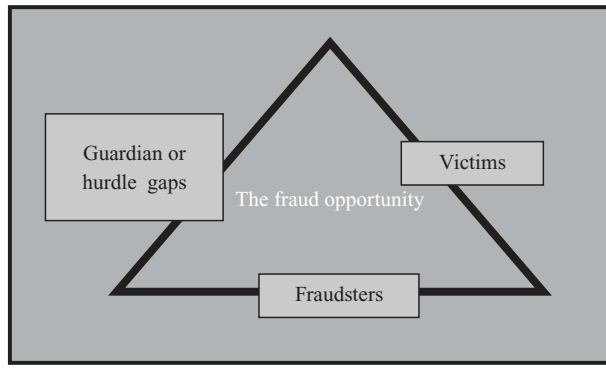

Figure 9.1 The crime triangle. (Source: Adapted from Clarke, R.V. (Ed.) (1997). Introduction. *Situational Crime Prevention*, 2nd edn. Harrow and Heston Publishers, Guilderland, NY, and Felson, M. (1998). *Crime and Everyday Life*, 2nd edn. Pine Forge Press, Thousand Oaks, CA.)

9.3.3 Selecting Countermeasures

A holistic, all-encompassing, interdisciplinary anti-counterfeit programme includes all aspects of a business, including design, intellectual property protection, manufacturing, inventory, distribution, retailing, use (possibly in resale) and disposal. The programme also includes many functions all along the product lifecycle. It is interesting – and important – to note that even the US FDA emphasised that anti-counterfeit systems work on verifying the package, not the product [16].

Some very basic questions should be asked before selecting new countermeasures when assessing overall risk. In many cases, there are basic work processes that could reduce the risk in the first place. Howard [17] proposed the following.

(a) Know your supply chain
    Do you know where you buy your supplies?
    Do you know where they buy their supplies?
    Do you formalise your relationships?
    Do you trust but verify?
    How much information do you supply others?
    Do you have long-term contracts?
(b) Know your channel(s)
    Do you know where your products are headed?
    Do you monitor where your products have been?
    Do those two statements match? Do you know?
    How many countries do you serve?
    Have you seen your products distributed?

Many brand protection experts will say ‘if you haven’t looked for counterfeits you can’t say you aren’t being counterfeited’.

In general, there are four functions in brand protection.

(a) *Product protection* includes actions on or in the product and package. These would include countermeasures for tamper resistance, child resistance, universal design/senior-friendly, cargo theft, shoplifting, return fraud, warranty fraud, expiration dates and recall efficiency.
(b) *Market monitoring* includes actions that look for anomalies or fake products in the marketplace, whether in a legitimate or illegitimate supply chain. Marketing monitoring functions are tied to product protection programmes.
(c) *Supply chain and channel integrity* covers actions that occur across a wide range of activities, including quality, but focuses on all who manufacture or move the product, including proprietary and contract plants, warehouses, shippers, distributors and retailers.
(d) *Enforcement and prosecution* includes actions to use laws and courts to catch, punish and stop fraudsters.

The entire system must be optimised to reduce the fraud opportunity in the first place, then to detect and deter.

To turn attention to assessing anti-counterfeit countermeasures, several practical questions are necessary [18]:

(a) Where is the product being compromised?
(b) Where will the product be verified?
(c) Who will verify it, using what methods?
(d) How will you use the results of the investigation?

To add to this set of questions, an optimal anti-counterfeit programme must include [13]:

(a) an understanding of how the counterfeit product is entering the marketplace
(b) the technical capabilities of the range of counterfeiters
(c) the capabilities and willingness of supply chain partners to partner in fighting the risk
(d) the capabilities and willingness of governmental enforcement
(e) consumers' awareness of the problem
(f) consumer willingness to participate in anti-counterfeit actions (e.g. consumer authentication).

All these assessments and programmatic recommendations emphasise assessing the current situation by first looking internally at standard operating procedures or even best practices that may be creating risks, assessing the fraud opportunity and then selecting countermeasures that can successfully answer the question: Are we disrupting the chemistry of the crime?

9.4 Anti-counterfeit Strategy: Components

Having covered aspects of anti-counterfeit strategy needed to determine specific countermeasures, we now turn to discussing the types of anti-counterfeiting

components. This section will provide an overview of the strategic functionality of countermeasures to provide an efficient way of understanding how to implement them. The section will cover the types of physical countermeasures of authentication and traceability, as well as an overview of the types of specific technologies available.

All countermeasures provide benefit operations for the brand owner or increased sales through an increase in consumer confidence. 'The operations function is some benefit that supports the inner workings of a company' [13]: this would be monitoring supply chain security or supply chain inventory level optimisation. 'The sales function is the feature increasing consumer confidence to support sales revenue' [13]: this would be anything that increases, or maintains, consumer confidence in the product, thus leading to sales revenue.

Before selecting any components, questions should be tightly framed. The questions for any new company or government anti-counterfeiting programme to address are as follows.

(a) Is the new system better at detection or deterrence of counterfeits than the current system?
(b) How *will* counterfeiters circumvent the system? (The increased cost or complexity of counterfeiting may become so high that the crime is diffused to other products or industries, or dissipated.)
(c) Is there a simpler solution that still accomplishes many of the benefits? For example, tracking of lots rather than individual units to find recalled or stolen products; in this case there is a cost–benefit advantage of decreased implementation costs with increased numbers of products recalled.
(d) How could the counterfeiters use harvested components to foul the legitimate supply chain (e.g. counterfeiters using authentic stolen, used or discarded components or codes)? Once counterfeits are co-mingled in the legitimate supply chain, even if they are eventually identified it is very difficult or impossible to un-co-mingle.

9.4.1 Functionality

Rather than general system-wide countermeasures, functionality should be selected to address a specific type of fraud and type of fraudster – some countermeasures may eventually be defined as thwarting many types of counterfeiters. It is important to use a 'surgical versus shot-gun approach' [19]. Anti-counterfeit countermeasures can be grouped by functionality. In most cases, countermeasures are a hybrid of many of the functionalities.

Some general terms and concepts are defined using ISO/DIS 12931 [11].

(a) Stand-alone or online connection: one operates by itself and the other must connect to a central system or database. A *stand-alone authentication tool* is an 'authentication tool which either is used to reveal a covert authentication element to the human senses for human verification, or which integrates the functions required to be able to verify the authentication element independently'. An *online*

authentication tool is an 'authentication tool which requires a real-time on-line connection to be able to locally interpret the authentication element'.

(b) Off-the-shelf or purpose-built: one is available commercially for many companies (including, presumably, high-tech counterfeiters) and the other is considered a 'trade secret' and built for one specific client. It should be emphasised here that all anti-counterfeit countermeasures have value relative to the specific type of fraud and fraudster – some very basic components are very effective especially in a multi-layered programme. An *off-the-shelf* authentication tool is defined as an 'authentication tool which can be purchased through open sales networks'. A *purpose-built* authentication tool is an 'authentication tool dedicated to a specific solution'.

(c) Human-readable or automated interpretation (also referred to as machine-readable): one can be read by a human without the aid of a special tool and the other can be read automatically, often at very high speed, by machine. *Automated interpretation* is where 'authenticity is evaluated automatically by one or more components of the authentication solution'. *Human interpretation* is 'authenticity as evaluated by the inspector'.

9.4.2 Types of Technology Solutions: Overt, Covert and Forensic

The types of anti-counterfeiting countermeasures apply to authentication and traceability, and are overt, covert and forensic:

(a) overt: 'authentication element which is detectable and verifiable by one or more of the human senses without resource to a tool (other than everyday tools which correct imperfect human senses, such as spectacles or hearing aids' [11]

(b) covert: 'authentication element which is hidden from the human senses, utilises the use of a tool by an informed person, reveals it to their senses or else allows automated interpretation of the element' [11]

(c) forensic: 'scientific methodology for authenticating material goods by confirming an authentication element or an intrinsic attribute through the use of specialised equipment by a skilled expert with special knowledge' [11].

The functionality of the countermeasures – authenticating or tracing – is identified as *continuous authentication* (ongoing, automatic function, on almost all the products) and *spot authentication* (occasional or incident-specific action) [13]. Continuous authentication is ideal since many products would be authenticated frequently. Spot authentication has a very valuable, and usually much more economically and practically reasonable, function since this allows testing when there is a concern or suspicious activity. Spot authentication can be implemented system-wide for all products or used on a sporadic basis to address a specific risk or to provide insight on a specific supply channel.

Planned obsolescence and multiple types and layers of countermeasures are critical. To continue to be effective, brand owners must continue to upgrade or replace anti-counterfeit countermeasures. If the product and brand are still in demand

and counterfeiting is still profitable, it must be understood that the bad guys will find a way to defeat or circumvent a technology. Furthermore, proving a product genuine or fake in court requires that confidential anti-counterfeit countermeasures need to be introduced as evidence; that measure is then publicly revealed and is no longer a trade secret.

9.4.2.1 Extrinsic and Intrinsic Characteristics

There are two general types of authentication and anti-counterfeiting characteristics, intrinsic or extrinsic.

An 'intrinsic [characteristic] refers to the authentication and anti-counterfeiting features contained in materials that are essential to an item, such as the paper and ink used to produce a banknote, or the board or plastic used in packaging' [20]. A more recent example is physical and chemical identifiers in the coatings of a solid oral dosage form medication, as noted in a draft guidance document issued by the FDA [21].

An 'extrinsic [characteristic] refers to devices or features which are produced offline and added to the document, product or packaging to make it more difficult to counterfeit. Examples include holograms, labels and now RFID chips' [20].

9.4.2.2 Inherent and Intrinsic Authentication

Inherent authentication is an often overlooked method that includes considering the uniqueness of a product or package system [22]. A packaging expert can review aspects of the package to compare the genuine and suspect product. For example, counterfeiters often use different or cheaper basic packaging materials such as solid unbleached sulphate (SUS) versus solid bleached sulphate (SBS) cartons. Another example would be different printing technologies used on the carton or labels. This has also been referred to as self-authentication [23].

This is different from the more precise and robust concept of intrinsic authentication, which has evolved to the stage where 'the unique characteristics of products or packaging are being used as a means of product authentication' [23]. More specifically, 'Technologies that fit this category are generically known as product fingerprinting and they are all based on the same premise: at the microscopic, molecular or nano-level the characteristics of every printed document, package or product are unique to that item' [23].

9.5 Authentication and Traceability Strategies

The terms authentication and traceability are sometimes used interchangeably but they are very different. There are even very different aspects to each of the terms themselves. One of those aspects is in how data gathered will be used. This can range from a quick internal identification all the way to use in court with very strict rules on the chain of custody.

9.5.1 Authentication

As of January 2011 and led by Technical Committee 247 Fraud Countermeasures and Controls (ISO TC 247), ISO became involved in anti-counterfeiting. The current draft standard ISO/DIS 12931 [11] includes working definitions of:

(a) *authentication* as the 'act of establishing whether a material good is genuine or not'
(b) an *authentic good* as a 'material good produced under the control of the legitimate manufacturer, originator of the good or holder of intellectual property rights'
(c) an *authentication tool* as a 'set of hardware and/or software system(s) that is part of an anticounterfeiting solution and is used to control of the authentication element'.

If the authentication feature is on a label or package then, technically, the authentication is not of the product but of the label or package.

The overall complexity of data collection and the monitoring of huge datasets create a challenge for authentication, but authentication also comes with other issues [13].

(a) Will consumers notice the absence of an authentication feature?
(b) With counterfeiters adding additional authentication features to trick consumers, would they notice the presence of a fake authentication feature?
(c) Will consumers become concerned with manufacturing variations in package or features? For example, would consumers perceive routine manufacturing variations as an indicator of a fake product?
(d) Will consumers consistently use the authentication features by, for example, looking closely at a hologram or submitting a serialised code for authentication?
(e) What is the potential impact of counterfeit awareness and authentication information on product marketing messages?

Authentication is often used because brand owners are seeking to either detect or deter counterfeiting by increasing their ability to confirm a product is genuine or to dissuade counterfeiters from attacking their products.

A key benefit of using authentication is the ability to prove a product genuine or fake, and dissuade counterfeiting.

9.5.2 Traceability

Traceability, or track and trace, is the ability to monitor where a product is going, where it has been and where it is right now – or to identify where it should not be. ISO/DIS 12931 defines track and trace as a 'means of identifying every individual material good or lot(s) or batch in order to know where it has been (track) and where it is (trace) in the supply chain' [11].

A traceability system includes a point where a code is read, is communicated to a central system where it is compared against a known product and then some

information is fed back to the source of reading. This is how a grocery store obtains the price of a product when the universal product code (UPC) barcode is read at the check-out. The code itself is just a data point. The interpretation of that data point by the central system communicates the information of what this is and how much it costs. This type of code is often referred to as a 'licence plate'.

With any critical data, there is a concern with security. There are numerous examples of even the most secure government and industry databases being compromised. If a set of all genuine codes was held in a single database and all those codes were harvested by a counterfeiter, the entire supply chain would become compromised. This breech could render the entire supply chain to be technically considered 'adulterated' by the US Food, Drug, and Cosmetic Act. The worst case must be considered where every database is vulnerable to attack, and mitigation crisis-management strategies must be considered for this vulnerability. Part of the crisis-management recuperability (the 'ability of system to recover from an attack') is back-up, redundant or multi-layered authentication systems [24].

There are many procedures for developing codes to trace products and many programmes to communicate the data (e.g. UPCs, GS1, EPC, etc.). The codes and systems are currently being addressed in proprietary, commercial, national and international standards bodies. A major concern with traceability is having the same code able to be used by all the supply chain partners. ISO/DIS 12931 defines this as *interoperability*, or the 'degree to which an authentication solution is able to work together with other different tools' [11]. Currently, the UPC system is an interoperable system that is used by almost all retailers in the USA.

Traceability is often used to comply with regulations, standard or required practice in industry, to meet competitor actions and, more generally, to reduce liability, increase supply chain optimisation and increase sales. During a product crisis, the traceability goal is to speed up the entire process or to reduce the number of products recalled: instead of recalling an entire supply of product, companies may be able to narrow the list to a much smaller group such as one batch or lot.

9.5.2.1 Pedigree

A more complex traceability function, which is intended to help with authentication, is pedigrees. The FDA defines a pedigree as the 'distribution history of a drug package' [16] – note that this specifically states the package and not the drug itself. With this definition of pedigree, each package would include a record of every owner and product movement from the Authorised Distributor of Record (ADR). In an electronic pedigree (e-pedigree) the history would travel on a device on the package. The ADR would keep records of the product they received. There are noteworthy and valid anti-trust issues with the pedigree system that have been held up in court [25].

9.5.2.2 Standardised Numerical Identification (SNI)

In March 2010, the FDA released *Guidance for Industry – Standards for Securing the Drug Supply Chain – Standardized Numerical Identification for Prescription Drug Packages* [26]. This was followed up with a workshop on drug tracking and tracing in February 2011 [16]. The guidance document is for the Food and Drug Administration

Amendments Act of 2007 (FDAAA) requirement that the FDA develop 'standards for identification, validation, authentication, and tracking and tracing of prescription drugs' and that the FDA 'shall develop an SNI to be applied to prescription drugs' [27]. The FDA clearly states that this is to be 'the first of several guidances and regulations' and that the guidance report 'contains nonbinding recommendations'. These are not mandatory. The recommendation is that the SNI be the serialised National Drug Code (sNDC) as set forth in Code of Federal Regulation 21 CFR part 207, with ten extra digits for additional identification of the product. The document also states that the sNDC is compatible with one of the most common international standards, the Global Trade Item Number (GTIN) established by GS1.

A key benefit of using traceability is being able to identify quickly where a product is, where it is going or where it should not be.

9.6 Overview of Technologies

Over the years, many excellent summaries of types of anti-counterfeit technologies and systems have been published; there is also a range of reports that summarise the technologies and markets. In 2011, Reconnaissance International partnered with Business Action to Stop Counterfeiting and Piracy (BASCAP) to produce an online reference database that is frequently real-time updated with oversight as well as technology updates. The list of technologies included in the Reconnaissance International Product Authentication and Security Database is shown in Table 9.3 [28].

Before selecting a technology and/or supplier, it is important to understand the functionality (e.g. stand-alone versus online authentication, etc.). Several other questions to consider could include the following.

(a) What does the solution do?
(b) How exactly does the solution detect and deter specific types of counterfeiters?
(c) How does it compare to what other people do? What are the other solutions or other suppliers of this specific solution?
(d) What are the benefits and drawbacks of those other solutions or other suppliers?
(e) How does it complement or compete with the company's current anti-counterfeiting or enterprise-wide systems?
(f) Is the solution ready to trial or implement immediately?
(g) How would those specific types of counterfeiters try to defeat or circumvent the system?
(h) Where has this technology been implemented before? What types of products, geography, breadth of implementation and does the supplier have press releases or references?
(i) How much does this cost to implement and manage? Are there any per-component unit costs?
(j) How is this solution sold or distributed? Does the supplier have control of their technology or could it be available to counterfeiters?
(k) Have they found their solution counterfeited? Have they looked?

Table 9.3 Authentication technologies. (Source: International Reconnaissance. (2011). The Product Authentication and Security Database. (www.pasdirectory.com). Accessed July 2011. Reprinted with permission from Reconnaissance International.)

Substrates & security components	• Security paper • Films, pressure-sensitive/tamper-evident laminates and label substrates • Security threads, tear tapes • Fibres, planchettes
Optically variable devices (OVDs)	• Hologram design, origination and production services and systems • Diffractive optically variable images (including holograms and kinegrams) • Reflective/refractive OVDs • Colour-shift optically variable films, foils and inks
Print technologies & features	• Security design software • Intaglio print systems • Security print features • Digital watermarks
Inks, pigments, coatings & taggants	• Ink components, additives • Coatings, lacquers, varnishes • Security inks • Taggants
Coding, fingerprinting, serialisation	• Coding and serialisation technologies • Fingerprinting
Integrators	• Security printers • Label converters
Support systems & services	• Consultancy • Internet monitoring • Investigation services • Analytical and verification systems
Legal services	

While the technologies are often brilliant and innovative, ‘zero cost technology’ (i.e. where a current system or process step can be adapted to provide an anti-counterfeit benefit) should not be overlooked. Many of the technologies presented can incorporate zero cost technologies or adaptations. It should be reiterated that for any anti-counterfeit countermeasure, the question to be asked, again, is: Are we disrupting the chemistry of the crime?

9.7 Conclusion

When considering anti-counterfeit countermeasures, the short-term objective is to mitigate current risks such as a known public health threat or infringement. The long-term objective is to reduce the overall vulnerability to future risks. This is often lost when focusing on operational risks rather than enterprise risk management. In counter-terrorism we do not ask an aeroplane pilot how many terrorist attacks have been stopped by having a reinforced cockpit door. In food safety we do not ask a plant manager how many food safety incidents they avoided by using a pathogen kill step. In retail store operations we do not ask a store manager how many slip and falls they avoided by mopping a spill. These are countermeasures that reduce the vulnerability, not just the risk of one type of attack. In the long run, this protects the enterprise.

A challenge when employees are very close to the problem and have first-hand experience with real people incurring real public health tragedies is how this risk fits into the overall risk appetite of the entire corporation. There may be other risks that often receive resource and financial priority – this is not to say that the risks at hand are not important. In other cases, the risk may be understood and prioritised, but the impacts of countermeasures are unclear or considered to not be effective. There are many risks that corporations consider 'catastrophic' and too unknown, too uncertain or too big to mitigate [29].

Anti-counterfeit strategy is not so complex when the fraud opportunity is deconstructed, when there is awareness of the specific types of fraud and fraudsters, when countermeasures are evaluated in direct relation to how they detect and deter specific attacks and when the overall enterprise risk appetite is understood.

Acknowledgement

This chapter was originally created for the Michigan State University (MSU) Anti-Counterfeiting and Product Protection Program (A-CAPPP) and is published here with the permission of the rights holder.

References

1. deKieffer, D. (2006). Trojan drugs: counterfeit and mislabeled pharmaceuticals in the legitimate market. *American Journal of Law & Medicine*. 32(2 & 3): 325–349.
2. European Commission. (2006). Summary of Community Customs Activities on Counterfeit and Piracy, Results at the European Border – 2006. (http://ec.europa.eu/taxation_customs/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/counterf_comm_2006_en.pdf). Accessed July 2011.
3. PriceWaterhouseCoopers. (2007). *Economic Crime: People, Culture and Controls*.
4. Spink, J. (2011). The challenge of intellectual property enforcement for agriculture technology transfers, additives, raw materials, and finished goods against product fraud and counterfeiters. *Journal of Intellectual Property Rights*. 16(2): 183–193.
5. Spink, J. and Moyer, D.C. (In press). New perspective for addressing the public health threat of

counterfeit medicines: a review of the Nigerian combating counterfeit and sub-standard medicines initiatives. *American Journal of Public Health*.
6. Spink, J., Helferich, O.K. and Griggs, J.E. (2010). Combating the impact of product counterfeiting. *Distribution Business Management Journal*. 10(1): 59–63.
7. Hagan, F. (2010). *Crime Types and Criminals*. Sage Publications, Thousand Oaks, CA.
8. Organisation for Economic Co-operation and Development. (2007). *The Economic Impact of Counterfeiting and Piracy, Part I: Overall Assessment*. OECD, Paris.
9. Spink, J., Singh, J.A. and Singh, S.P. (In press). Review of package warning labels and their effect on consumer behavior with insights to future anti-counterfeit strategy of label and communication systems. *Packaging Technology and Science*.
10. Spink, J. and Moyer, D.C. (In press). Defining the public health threat of food fraud. *Journal of Food Science*.
11. International Standards Organization. (2011). ISO/DIS 12931: Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods. ISO, Geneva.
12. Department of Justice/US Drug Enforcement Agency DEA. (2010). OxyContin. (www.justice.gov/dea/concern/oxycontin.html). Accessed July 2011.
13. Spink, J. (2009). What role can we count on consumers to play in authentication? Anti-Counterfeiting and Product Protection Program (A-CAPPP) Paper Series 1–35. (www.a-cappp.msu.edu/publications.html). Accessed July 2011.
14. Clarke, R.V. (Ed.) (1997). Introduction. *Situational Crime Prevention*, 2nd edn. Harrow and Heston Publishers, Guilderland, NY.
15. Felson, M. (1998). *Crime and Everyday Life*, 2nd edn. Pine Forge Press, Thousand Oaks, CA.
16. United States Food and Drug Administration. (2011). *Determination of System Attributes for the Tracking and Tracing of Prescription Drugs: Public Workshop*. US FDA, Silver Spring, MD.
17. Howard, D. (2008). *Traceability Is Not Authentication – The International Authentication Association Manifesto*. 4th Global Forum on Pharmaceutical Anti-Counterfeiting. (www.internationalauthenticationassociation.org/upload/file/IAA%20GF4%20Jun08.ppt#378,13, Understanding Your Company). Accessed July 2011.
18. McNeely, S. (2005). *Partnerships with Security Product Suppliers*. Paper presented at PIRA Innovations in Security Technology Conference, Chicago, IL.
19. Ryan, R. (2011). *Food Safety Modernization Act*. Paper presented at FBI International Symposium on Agro-Terrorism, Kansas City, MO.
20. Authentication News. (2006). Intrinsic characteristics for authentication. *Authentication News*. 12(7): 7.
21. United States Food and Drug Administration. (2009). FDA-2009-D-0212: Draft guidance for industry on 'Incorporation of Physical–Chemical Identifiers into Solid Oral Dosage Form Drug Products for Anticounterfeiting'. *Federal Register, Department of Health and Human Services, Food and Drug Administration*. 74(133): 34021–34022.
22. Spink, J. (2010). Graduate Course Curriculum: VM/CJ 840 Anti-Counterfeit and Product Protection. Michigan State University, East Lansing, MI.
23. Authentication News. (2010). Intrinsic authentication and traceability. *Authentication News*. 16(5): 6–7.
24. Center for Food Safety and Applied Nutrition. (2007). CARVER + Shock Software Tool. US FDA CFSAN. (www.fda.gov/Food/FoodDefense/CARVER/default.htm). Accessed July 2011.
25. Tesoriero, H.W. (2006). Injunction delays part of anti-counterfeit drug law. *The Wall Street Journal*. 4 December 2006, p. A12.
26. United States Food and Drug Administration. (2010). *Guidance for Industry, Standards for Securing the Drug Supply Chain – Standardized Numerical Identification for Prescription Drug Packages, Final Guidance*. US FDA, Silver Spring, MD.
27. United States Food and Drug Administration. Food and Drug Administration Amendments Act (FDAAA) of 2007. (www.fda.gov/RegulatoryInformation/Legislation/federalfooddrugandcosmeticactfdcact/significantamendmentstothefdcact/foodanddrugadministrationamendmentsactof2007/default.htm). Accessed July 2011.

28. International Reconnaissance. (2011). The Product Authentication and Security Database. (www.pasdirectory.com). Accessed July 2011.
29. Taleb, N.N. (2007). Black swans and the domains of statistics. *The American Statistician*. 61(3): 198–200.