Chapter 10
Supply Chain Management (Part 2 of 2): Application Applied to Food Fraud Prevention

Summary

This chapter presents the application of supply chain management practices to food fraud prevention. There are SCM systems that are created to address current concerns and also to comply with laws, regulations, certifications, standards, and common practices. This chapter will expand on the previous review of the SCM fundamentals and address several key application challenges as well as the presentation of some specific studies. Since food fraud prevention is currently being developed and implemented, it is opportune to review the broader business application as well as specific insight from other industries.

The Key Learning Objectives of this chapter are

- (1) **Supply chain management application to food fraud prevention**: How this discipline applies to food fraud prevention practices.
- (2) **Traceability and electronic transactions**: Explore key concepts and standards related to traceability, transparency, and the opportunity for new enhanced traceability technologies.
- (3) **Review of previous enhanced traceability efforts**: Then to review details of several supply chain traceability projects or initiatives.

On the Food Fraud Prevention Cycle (FFPC), this chapter addresses the theoretical foundation concepts related to supply chain management in "(A) Academic Disciplines" (Fig. 10.1).

J. W. Spink, *Food Fraud Prevention*, Food Microbiology and Food Safety,
https://doi.org/10.1007/978-1-4939-9621-6_10

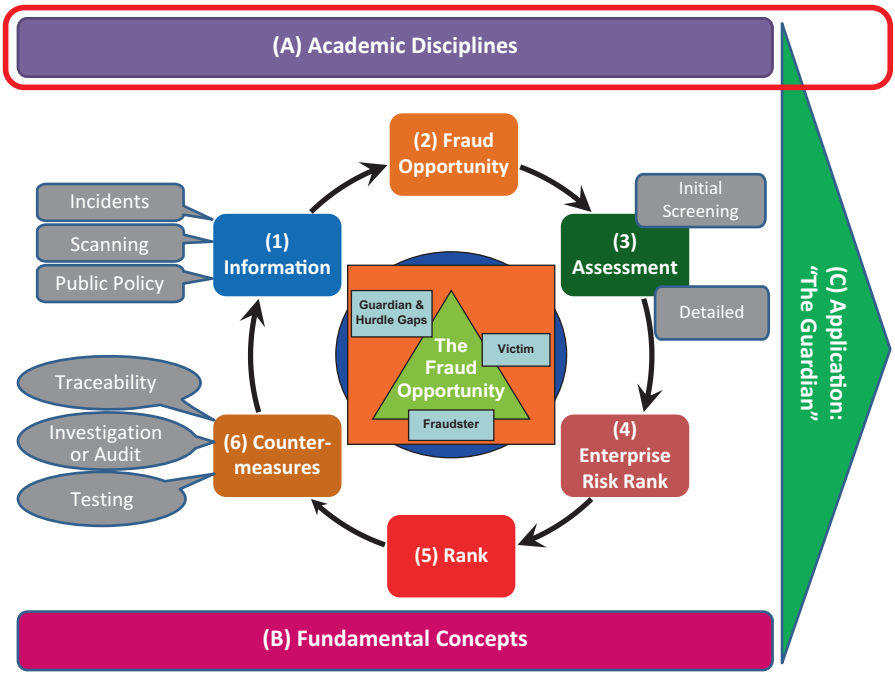

Fig. 10.1 Position on the Food Fraud Prevention Cycle: Where this chapter applies to the overall concept "(A) academic disciplines". (Copyright Permission Granted) (Spink 2014; Spink et al. 2019)

Introduction

Supply chain management developed as a separate business school research discipline after there were examples of added value and explanation of an unmet need. As the terminology and value became clearer, the discipline kept evolving and rising in importance. Food fraud may be undergoing that type of evolution as a separate research discipline including with the direct application to supply chain management. Beyond the fundaments – of both food fraud and supply chain management – the value is explained through the application and synthesis of the academic disciplines. This chapter builds upon the previous food fraud prevention concepts and the preceding supply chain management fundamentals chapter to explain the application.

Key Learning Objective 1: Supply Chain Management Application to Food Fraud Prevention

This section reviews the food fraud prevention communication and integration into a supply chain management operation.

The Key Learning Objectives of this section are:

- (1) Understanding the current internal controls
- (2) Exploring the specific laws and regulations that apply to supply chain controls
- (3) Then reviewing the role and opportunity from enhanced traceability

Supply Chain Laws and Regulations

Laws or regulations are formal requirements, and they are supported by a range of programs or collaborations including standards.

The laws that govern the food supply chain are based on the food regulations (the production and consumption of the product) or supply chain-related regulations (the movement of the goods). The food laws in the USA include the Food, Drug, and Cosmetics Act (FDCA) and the Food Safety Modernization Act (FSMA). In addition, there are broader laws that cover smuggling, the safe transit of products, driver, and equipment requirements, as well as addressing stolen goods. For example, an FDA-administered law for drugs is the US Drug Supply Chain Security Act (DSCSA) which provides guidelines for compliance and consequences for the stolen product including considering the entire batch or lot unfit for commerce until the suspect product is identified and removed.

There are programs or collaborations from many governments, nongovernmental organizations (NGO), nonprofit organizations (NPO), nonprofit corporations (NPC), or industry initiatives (IRS 2018) (see Table 10.1). All programs provide additional transparency of the supply chain even though they often do not prioritize food or non-terrorism activities. In some cases, the focus on terrorism or public health issues shifts resources or focus from general activities and could actually create a new "fraud opportunity" for food fraud prevention.

- ***For food fraud prevention***, an intense focus on pharmaceuticals, high-volume product counterfeiting, and weapons of mass destruction leads to fewer resources or prioritization of incidents such as nonpublic health-related food fraud.

There are a range of standards created and adopted including from industry organizations or international nongovernmental organizations (see Table 10.2) (for more, see chapter appendix).

Next, there is a range of ISO activities in security management and product fraud that apply to the Food Fraud Prevention Strategy (Table 10.3).

A key to all the laws and regulations is an expected level of supply chain traceability and the ability for transparency. Frequently there is even an assumption that traceability and transparency are a "given."

Table 10.1 Review of US and global supply chain security programs

Title	Authority	Focus	Goal	Application to food fraud
Customs-Trade Partnership Against Terrorism (C-TPAT)	US Customs	Protecting the US market from terrorism and specific products imported to conduct the act	To increase the efficiency of identifying opportunities and to target inspection resources. Approved vendors can have more rapid border crossings	Additional transparency of the supply chain
Standards to Secure and Facilitate Global Trade (SAFE Framework)	World Customs Organization (WCO) (created within what would become the OECD)	Same as C-TPAT but global focus	To connect international trade communication to disrupt terrorist shipments	Same as C-TPAT. Note: the "SAFE framework" is different from the food-related "SSAFE Organization"
Partnership in Protection (PIP)	Canadian Border Services Agency	Combating terrorism but also organized crime, contraband, and other smuggling	Increase inspection effectiveness through voluntary collaboration. Similar requirements at C-TPAT	Food fraud would be one of the focus areas under smuggling, contraband, and counterfeiting
FAST (Free and Secure Trade)	US Customs (CBP) and Canada Border Services Agency (CBSA)	Facilitate US-Canada trade and inspections.	Increase inspection effectiveness through voluntary collaboration. Similar requirements as C-TPAT	Food fraud would be one of the focus areas under smuggling, contraband, and counterfeiting
AEO (Authorized Economic Operator)	European Community Customs Code (Regulation [EC] 648/2005)	Facilitate and streamline commerce across borders	Faster border crossings	Transparency of harmonized information exchange
CCSP (Certified Cargo Screening Program)	US Transportation Security Administration (TSA)	Explosives on airplanes	Protect against terrorist attacks	Some additional transparency. Resources could monitor for fraudulent activity
PCSC (Pharmaceutical Cargo Security Coalition)	NGO, similar membership as RX-360 and Pharmaceutical Security Institute (PSI)	Shared intelligence activity to secure products in the supply chain and especially large shipments such as container loads	Focus on pharmaceutical stolen goods, specifically full container (truckloads, shipping containers, etc.)	No direct application except insight on best practices

(continued)

Table 10.1 (continued)

Title	Authority	Focus	Goal	Application to food fraud
TAPA (Transportation Asset Protection Association)	An NGO organized by industry	Increase supply chain security of high-tech material and goods	A focus is on pharmaceuticals	Transparency of the entire supply chain. Resources could monitor fraudulent activity

Adapted in part from Arway (2016)

Table 10.2 Review of standards that apply to food fraud or related products

Title∗	Authority∗	Focus	Goal	Application to food fraud
ISO 9000 Quality Management	International Standards Organization (ISO), Technical Committee 76 Quality management and quality assurance, Sub-committee 1 Concepts and terminology (SO/TC 176/SC 1)	General business practices that streamline operations and reduce product specification anomalies. As ISO 22000 is the base for food safety management systems, ISO 9000 is the base for quality management systems	Increase the quality of the product produced and distributed	Food fraud is a component of product quality
ISO 28000 Supply Chain Security	International Standards Organization (ISO), Technical Committee (TC) 292 Security and resilience	Specifies security management of the products as they move through the supply chain, including control facilities and in route	"a) establish, implement, maintain and improve a security management system; b) assure conformance with stated security management policy; c) demonstrate such conformance to others; d) seek certification/ registration of its security management system by an Accredited third-party Certification Body; or"	This supports control of the products as they move into, through, and out of the controlled legitimate supply chain. The ISO 28000 practices can reduce or increase the fraud opportunity

(continued)

Table 10.2 (continued)

Title∗	Authority∗	Focus	Goal	Application to food fraud
ISO 27000 Information Security	International Standards Organization (ISO), Joint Technical Committee JTC) 1 Information technology, Sub-Committee 27 IT Security techniques (ISO/JTC1/WC27)	Protect information from attack or unauthorized access	Reduce risk from attacks and the potential illegal accidental disclosure of information	Protects the integrity of traceability and authenticity databases
ISO 22000 Food Safety Management	International Standards Organization, Technical Committee 34 Food products, Sub-Committee 34 Management systems for food safety (ISO/TC 34/SC 17)	Health hazards from food safety incidents	Reduce health hazards and increase the methodology to reduce the possibility of incidents	Focuses on health hazards, new food fraud requirements in 2018
ISO 22380: 2018 (previously ISO 19564) Product Fraud: Product fraud countermeasures and control – General principles	ISO TC292/WG4, focused on product fraud prevention management methods and systems.	Broadly addressing product fraud for all material goods and presenting basic principles and terminology	Enable harmonization and sharing of best practices by establishing a common terminology and basic prevention focused principles	Specifically addresses product fraud and food fraud. Includes methods to assess and address
ISO 12931:2012 Performance criteria for authentication solutions used to combat counterfeiting of material goods	International Standards Organization (ISO), Technical Committee (TC) 292 Security Management and Resilience (ISO TC 292/WG4)	Management of authentication features to detect or prevent fraud acts	Offer common and optimized countermeasures to provide holistic industry response	This provides insight and best practices from other material goods as well as provides a common terminology and methods for foods
ISO 22380: 2018, Section 4.5.1 Profiling product fraud	ISO 22380, section on the organization of incident information	Specifically, this adapts and synthesizes other best practices to present a simple and codified method for organizing incident information (see the PCICT section)	Same as ISO 22380	

(continued)

Table 10.2 (continued)

Title∗	Authority∗	Focus	Goal	Application to food fraud
ISO 22380: 2018, Section 4.5.2 Risk assessment	ISO 22380, section presents a method to plot risks on a heat map (similar to ERM/COSO)	To enable calibrating a new product fraud risk with all enterprise-wide risks, this presents a method to create a single heat map	Same as ISO 22380	
GFSI (Global Food Safety Initiative)	Member organizations under the Consumer Goods Forum.	Defines expectations of a food safety management system	Reduce the opportunity for food safety issues including explicitly addressing the root cause of food fraud	There are direct requirements including a vulnerability assessment and prevention strategy
Business Alliance for Secure Commerce (BASIC)	An NGO organized by industry.	Create standards and common business practices	Increase the efficiency of transactions including information technology interoperability	Transparency of harmonized information exchange

Excluding the standards that are not supply chain specific such as the ISO product fraud and authentication noted above

Table 10.3 Review of ISO product fraud and related standards (ISO 2017)

Published	
ISO 12931:2012	**Product fraud**: Performance criteria for authentication solutions used to combat counterfeiting of material goods
ISO 16678:2014	**Product fraud**: Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade
ISO 22300: 2018	**Security and resilience**: Terminology (not to be confused with the ISO 22000 Food Safety Management series) (developed in parallel with other material goods product fraud standards ISO 22380, ISO 12931, and ISO 16678))
ISO 22380:2018 (formerly ISO/CD 19564)	**Product fraud**: Security and resilience (authenticity, integrity, and trust for products and documents)—general principles for product fraud risk and countermeasures
ISO 28001:2007	**Security management systems for the supply chain**: Best practices for implementing supply chain security, assessments, and plans—requirements and guidance
ISO 28002:2011	**Security management systems for the supply chain**: Development of resilience in the supply chain—requirements with guidance for use
ISO 28003:2007	**Security management systems for the supply chain**: Requirements for bodies providing audit and certification of supply chain security management systems
ISO 28004-1:2007	**Security management systems for the supply chain**: Guidelines for the implementation of ISO 28000 (Part 1: General principles)

(continued)

Table 10.3 (continued)

Published	
ISO 28004-3:2014	**Security management systems for the supply chain**: Guidelines for the implementation of ISO 28000 (Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses) (other than marine ports)
ISO 28004-4:2014	**Security management systems for the supply chain**: Guidelines for the implementation of ISO 28000 (Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective)
Underdevelopment	
ISO/DIS 34001.4	**Product fraud**: Security management system for organizations assuring authenticity, integrity, and trust for products and documents
ISO/NP 22383	**Product fraud**: Security and resilience (authenticity, integrity, and trust for products and documents)—performance criteria for authentication solutions used to ensure genuineness and integrity of material goods
ISO/WD 22384	**Product fraud**: Security and resilience (authenticity, integrity, and trust for products and documents)—guidelines to establish and monitor a protection plan and its implementation
Not TC292 but related	
ISO/IEC 27000:2016	**Information technology**: Security techniques (information security management systems, overview, and vocabulary)
ISO/IEC 27001:2013	**Information technology**: Security techniques (information security management systems, requirements)
ISO/IEC 27002:2013	**Information technology**: Security techniques (code of practice for information security controls)

Sidebar: The Assumption of Traceability and Transparency as a "Given"

The assumption of supply chain traceability and transparency is a new and evolving concept that is challenging. It appears that the ability to monitor and identify the location of products is accepted as a "given." The concept of monitoring for the rogue product—e.g., "and to prevent the introduction to the supply chain of unauthorized contraband" which is different than "*authorized* contraband"—is only mentioned as an odd or future consideration. (Product counterfeiting and other related activities are currently considered to be under the management of corporate security or brand protection.)

Sidebar: The Role of the "Brand Protection Manager" in Food Fraud Prevention

Expanding on the Brand Protection Manager concept and their role in food fraud prevention, an excerpt from (MSU FFI 2017):

> Food fraud sounds like a responsibility for food scientists or purchasing agents. Brand Protection managers – usually focused on finished goods activities such as

diversion, illegal re-packaging, expired or sub-standard product, and counterfeiting – often are not responsible for ingredients or more operational problems. Due to the nature of fraud that does *not* include ingredients or adulterant-substance, in many cases, the Brand Protection manager may be the first one to identify the threat as product fraud. They will probably be the first to recognize preventative controls that *should* be applied by their accountable corporate CEO but probably not responsible in their own workgroup. Brand Protection managers have a unique skill set and experience that is critical to identifying, describing, and to help prevent or mitigate food fraud. Beyond FSMA, FDA has an expanding scope that covers cosmetics, personal care products, pet and animal food, tobacco, and alcohol so many "consumer products" Brand Protection managers are accountable for food fraud… whether they know it or like it.

Key Learning Objective 2: Traceability and Digital Transactions

This section reviews the traceability fundamentals and related electronic transaction products and services. A strategic approach considers the basic specification of the requirements in relation to what can be expected.

The Key Learning Objectives of this section are:
- (1) The role of traceability in food fraud prevention
- (2) The importance and benefits of supply chain transparency
- (3) Review of several application examples

Traceability and Electronic Transactions

Supply chain management has advanced as a discipline in part due to the ability to gather a tremendous amount of data, more real-time insight on buying and transportation of products, computing power such as global positioning, web and mobile communication, and the massive power of the computers themselves. With more information, there is more opportunity for more visibility of the entire supply chain including traceability, track and trace, and transparency.

- ***Traceability (ISO)*** is defined as where the product is, where it is going, and where it has been. A similar phrase ***track and trace*** is defined by ISO 12931 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" (Note: ISO 12931 states "Track and Trace technology when used alone is not considered to be an authentication solution" (ISO 2011)).
  - ***Track (ISO)***: where a product has been
  - ***Trace (ISO)***: where a product is going

The GS1 standards provide a similar but alternate set of definitions (GS1 2018a, b):

- **Trace/tracing (tracing back) (GS1)**: "The ability to identify the origin, attributes, or history of a particular traceable item located within the supply chain by reference to records held" (GS1 2018a, b).
- **Track/tracking (tracking forward) (GS1)**: "The ability to follow the path of a traceable item through the supply chain as it moves between parties" (GS1 2018a, b).
- **Traceability (GS1 references ISO 9001)**: "is the ability to trace the history, application or location of that which is under consideration" (GS1 2018a, b).

When reviewing these concepts, there is a realization that there is a higher goal which is visibility of the entire set of all transactions:

- ***Transparency (GS1)*** is "defined as visibility of products and transactions throughout the supply chain" (GS1 2007). A similar concept *supply chain visibility* is defined as "location and status of supply chain inventory and resources" (Bowersox et al. 2002).

There are many ways that a company tracks or monitors products such as electronic invoices or interacts with consumers such as frequent shopper rewards. Any and all monitoring of the product increases the visibility of the flow as well as increases transparency. The electronic invoices already carry a lot of information about many aspects of the shipment and product as well as offering very high reliability and quickly accessible information. A receiving company monitors and confirms the physical shipment before accepting—and then paying—the invoice.

For food fraud prevention, the application is that two of the most intensely scrutinized supply chain handoffs are when there is a financial exchange (e.g., paying an invoice). This intense scrutiny is an opportunity for either inspecting or authenticating product as well as for electronically interacting with the pallet or case as well as the actual final consumer package. Barcode readers or scanners could provide additional functions such as to authenticate the product (actually this type of authentication confirms the label is correct, and it is assumed that the product inside the package is genuine).

The data security and information validity requirements are less stringent for supply chain management (trying to move product around to fill store shelves) than for food safety (stopping shipments before consumers ingest dangerous product) and for food fraud prevention management (providing assurance that the product is still genuine and has not been tampered with). For food fraud prevention, some criminals would benefit from hacking into the databases. Illegal and unauthorized access to databases could enable the uploading of fraudulent codes that would be then confirmed to be authentic, to the unauthorized release of products such as inventory, confirm that tax payments have been made, establishing that refunds should be paid, or confirming that shipments have already been inspected, or others.

The supply chain management focus is making sure the right product is in the right location to allow for a sale, while the food safety focus is finding the product to stop shipment or product recall. For food fraud prevention, there is an additional value or requirement to track the product once it enters the supply chain (assuming or checking authenticity at that entry point) and then monitoring the product through often many handoffs until delivering to the buyer or user.

Sidebar: Does Traceability Really Help Fight Fraudsters? (MSU FFI 2018)

Title: Does Traceability Really Help Fight Fraudsters?

By John Spink • May 29, 2013 • Blog

Traceability – finding where the product has been, where it is going, or where it is right now – is increasing in importance for the food industry for a number of reasons. Authentication – proving the product genuine or proving it fake – is also increasing in importance, especially when combined with traceability within the supply chain, which reduces the fraud opportunity. Together traceability and authentication provide transparency. When there is improved transparency, the Food Safety, Food Defense, and food fraud risks can be minimized.

Traceability initiatives have different benefits for different objectives:

- Food Safety – Minimizing Consumption of Suspicious Product. There have been calls from agencies and industry for improving traceability of the food supply chain. This is reiterated and defined further in the Food Safety Modernization Act (FSMA, the law itself) that was passed in January 2011 and is supported by draft rulemaking (how FDA will implement the law).
- Food Defense – Stolen Goods. The FDA has released a response to cargo theft that includes mandates for companies to be able to identify specific stock-keeping-units that have been stolen. If the company cannot identify the specific product that was stolen – and out of their control – then the company will need to recall all product in the smallest lot identifiable. For example, if three batches of products are in a load of stolen goods, then all of those lots will need to be recalled. To my knowledge this has not been implemented…but it could.
- Food Defense – Attack for Harm. The attack on the supply chain, specifically adulterating a food product with a contaminant that causes harm, is of particular interest to FDA. The FDA Food Defense directives leverage the transparency provided by the other food safety-related regulations.
- Food fraud – Identifying Suspicious Product. Food fraud is deceptive use of food for economic gain which is illegal in the US under the Adulterated Foods and Misbranded Foods sections in the Food, Drug & Cosmetics Act.

(continued)

The fraud opportunity is significantly reduced with increased transparency of ingredients moving through a long supply chain. As mentioned, the transparency is created by traceability and authentication.

These concepts are supported by the Institute of Food Technologists, the Global Food Safety Initiative, the Produce Marketing Association, and the International Association for Food Protection.

The concept of food traceability contributing to food fraud prevention is something that I included in the MSU-FFI public comments at an FDA public meeting in 2009. The MSU-FFI public comments were:

- Include food fraud considerations in the FDA traceability initiative as you include both food safety and food defense.
- Consider traceability programs integrated across all FDA regulated products including drug, medical device, food, cosmetics, and then all consumer products.
- It is my opinion that retailers and retail inventory management systems are a crucial supply chain node since this is the last transaction – scanning at checkout – before the product leaves the distribution system and is transferred to the consumer.

So, traceability is not a single magic bullet to stop fraud, but it is a critical part of the food fraud prevention system. Traceability and authentication provide transparency within the supply chain which reduces the fraud opportunity. If you review the MSU-FFI past blog posts, you'll see examples of how bad guys not only circumvent our protection systems but in some cases, even use them against us. Whether it is more active tracking of lot numbers, or expanding to unit-level serialization, traceability has a vital role in increasing transparency and in product protection. What you need to do is consider how a tactical program to track your products can become a strategic deterrence countermeasure. MSU-FFI.

Sidebar: Will Supply Chain Transparency Reduce Food Fraud? Sure, They Must, Don't They?

There is a saying:

> *General countermeasures generally help; specific countermeasures specifically help.*

Unless there is a regulatory requirement, a specific proposal is required for financial or human resource expenditure. To review the value of a countermeasure or control system, a very specific question must be identified. Many supply chain transparency or anti-counterfeiting proposals stall because the final resource allocation decision-maker either can't prioritize or justify this specific

expenditure. A basic ROI would compare this allocation versus all other ROI proposals including examples such as hire a new sales representative, spend more on advertising, fix a piece of manufacturing equipment that is leaking, conduct discretionary maintenance, purchase a new piece of food safety testing equipment, or even address other risks. Even a specific ROI for a regulatory requirement—now only comparing proposals to address this risk—requires a level of confidence in the success of the proposal to meet the goals efficiently.

The Max Bazerman concept of "best alternative to a negotiated agreement" (BATNA) may be to "do nothing" (Bazerman 2001). For new technologies, it is often a better decision to be a "fast follower" than an "early adopter" (Porter 1985; Makadok 1998; Dietrich et al. 2006; BRIDGE 2007; Voss et al. 2009; Anthony 2012). "Manufacturers and distributors wanted to avoid being the early adopter, preferring to be a 'fast follower' with EPC/RFID [Electronic Product Code-based Radio Frequency Identification for brand protection and anti-counterfeiting]" (HDMA 2004).

To provide an example of the preference of being a "fast follower," interoperable enhanced traceability has been a holy grail for solution providers. *Interoperable* refers to the ability for systems to interact and share information freely such as all supply chain partners using the same coding system such as the GS1 Global Trade Item Number (GTIN), universal product codes (UPC), or others (Bix et al. 2007; ISO 2017; GS1 2018a, b). "Enhanced" in this example refers to more standard and more capable systems. Finally, *traceability* is being able to track or trace product which could include where it is, where it has been, and where it is going, among others (ISO 2005)). Together the interoperable enhanced traceability is a more robust product tracking system that includes a lot of information that is shared quickly and easily (we did not say "freely" because each activity usually includes fees such as for the use of the codes, storage, and retrieval of the data, analysis of the data, use of patented algorithms or computer programs, and the ongoing information technology computer support).

Sidebar: Enhanced Traceability Systems such as Barcodes, Mass Serialization, Pedigree, RFID, Transaction Security, Encryption, and Others

Whether the traceability enabler is one-dimensional barcoding (1-D), two-dimensional barcoding (2-D including QR codes), mass serialization, radio-frequency identification device (RFID) or automatic identification (Auto-ID), transaction security, and so on, there is a long list of magic bullet ideas. To consider the practical and pragmatic value of a new technology, there are some possible questions to consider:

(continued)

1. Is more traceability good? Sure.
2. Does more traceability improve transparency of the supply chain? Absolutely.
3. How soon will it be implemented to 95%—or even 50%—of a company's entire supply chain? To be determined.
4. How much will it cost to implement? This could include preparing current IT systems to communicate with the new program, to enable the proprietary supply chain to interact, and to encourage and enable the upstream and downstream supply chain to interact any ongoing cost for the use of the codes, data storage, data retrieval, data analysis, and then ongoing management. To be determined. Millions? Tens of millions? Hundreds of millions?
5. How much will the interoperable enhanced traceability contribute to the bottom line? To be determined.
6. How does this interoperable enhanced traceability specifically reduce a unique type of fraud opportunity? Unknown.
7. "If one aspirin is good then ten is better? Right?" Not necessarily and usually "no."
8. So far the interoperable enhanced traceability sounds promising, but there has not been a very compelling—or any—business case… *at least not yet*.

Often the recommendation or justification for adoption explains the "features" of the technology or system (e.g., the difficulty of a security product copied) with details of the severity of the overall problem (e.g., food safety product recalls create health hazards) but little on the exact "benefit" of how the specific fraud opportunity will be specifically reduced.

Sidebar: New Enhanced Traceability Technology and the Horsemeat Food Fraud Incident

The horsemeat food fraud incident has been reviewed and analyzed widely. Essentially the brand owner made their routine order to replenish packaged product from their manufacturer. A series of bids and proposals worked their way to a meat producer. The meat producer shipped the blocks of frozen raw meat to the manufacture, and the lasagna was made, packaged, shipped to the original customer, and then placed on the retail shelves in the UK. The meat was monitored for quality and food safety. Records were reviewed, kept, and all passed inspection. No one was assigned to check for the correct species.

This is a very specific food fraud incident that provides valuable insight into assessing and judging countermeasures and control systems. This is one type of food fraud, so it is an excellent case study to review the value of enhanced traceability technology.

The meat producer was a recognized and approved supplier, so they were considered a trusted and verified supply chain partner. The seller and purchaser are very formally and visibly connected through the invoice, inventory management, and accounts payable systems. The meat supplier in many cases has been audited by a certification body or even by the brand owner itself. This point of trust—human intervention—is where the fraud occurred.

So, considering that an approved, trusted, and verified supplier is a point of trust is actually a vulnerability, this is a specific point in the supply chain to consider that an additional specific countermeasure and control system can be considered. One type of risk treatment would be traceability or transparency. With enhanced traceability technology, the transactions and documents passed along are not able to be altered but only updated with a record of what was changed and by whom (assuming additional identity theft has not occurred—see your email spam folder for fraudulent emails from the URL of "your bank"). There would be less of a fraud opportunity to enter falsified claims if there is a check further down the supply chain. For example, the lasagna manufacturer or brand owner could occasionally conduct a species authenticity test and enter that into the traceability system. This would both identify the food fraud incident and reduce the fraud opportunity since the fraudster would know there is a higher chance their crime would be caught (assuming there is no fraud or bribery occurring at the brand owner itself).

When considering the overall countermeasures and control systems, it is logical that species authenticity tests should be conducted. If the new tests are publicized in a way that the fraudsters can be aware of the change, then there will be a decreased fraud opportunity. (If the fraudsters don't know about your new test, then you will just catch more fraud and not achieve the real goal to prevent it from occurring in the first place.) It would be logical that the fraudsters will consider how to adapt their operations such as to change fraudulent methods, attack someone else, or stop conducting the crime (this is "crime displacement"). A question is whether the enhanced traceability technology system is—or how much more—valuable than the current tracking systems. To be determined. With this further review of a specific incident, there can be a specific assessment of enhanced traceability technology versus current or alternate systems.

Key Learning Objective 3: Reviews of Past Traceability Efforts Including the California Drug Pedigree and RFID

This section reviews several past traceability efforts related to radio-frequency identification devices (RFID) and drug pedigree laws. There are many best practices and lessons learned from many past effort that were successful… and maybe even *more* value from closely reviewing the efforts that did *not*.

The Key Learning Objectives of this section are:

- (1) Information database security and accuracy
- (2) Review of an RFID project
- (3) Review of drug pedigree and specifically the California efforts

Information and Database Security: Hackers Adding Fake Codes

Databases are only as good as the data in the system. There is a saying "garbage in, garbage out" which means that if the information being entered is not accurate, precise, or certain, then the results or conclusions will also be problematic. Another concept is that data systems have a tendency to gravitate toward chaos. A data set should be expected to develop problems or inconsistencies. An important concept is how to reconcile or correct errors, mistakes, or flaws. The idea that a data set could be imperfect is a point *not* understood when considering anti-counterfeiting systems such as validating the code on a medicine package in the surgical suite before (trying to) restart someone's heart. In that setting, if reading the code to confirm authenticity, then the acceptable reliability of the data set is far *below* 1% or maybe probably below 0.1%. An important consideration is that most data sets are probably not accurate below 1% (if not much less accurate).

If a traceability or authentication system is used as the definitive method to recognize or approve products, then there is a tremendous fraud opportunity incentive for hackers to disrupt, corrupt, or co-opt the database. For example, if fake, duplicate, or nonsensical codes were entered, then the confidence in the entire database would be undermined. Also, there would be an incentive for hackers to upload counterfeit codes, so future authentication queries would confirm the counterfeit code and product to be "genuine."

Another consideration is that fraudsters could flood the database with nonsensical codes, so the number of errors requiring correction would be so high (e.g., hundreds, thousands, more?) that reconciliation and correction would be impractical. The flooding of a database with nonsensical codes could undermine the value of the database, itself. Although not a database, there are examples of entire systems being undermined by errors. In 2005, the entire US supply of the very popular cholesterol drug Lipitor was recalled—sales were halted—since the unapproved product had been comingled and could not be immediately un-comingled. It would seem it was less risky for the supplier to recall the entire US supply of product rather than trying to sort which product was good or bad.

Also, during discussions about the US Prescription Drug Marketing Act of 1987 (PDMA)—still not fully implemented in 2017—and the California State Bill 1976 (SB-1476) California E-Pedigree Law, there were later discussions that possibly the credit card industry had database security that would apply (CSBP 2007, 2012, 2013). It was not mentioned that the credit card industry databases are frequently

hacked and there is an allowance for stolen or corrupt credit card numbers. (Note: Remember that credit card companies encourage consumers to review their credit card statements for fraudulent or incorrect transactions that are usually instantly credited.) While a 3% error or fraud rate for a credit card may be acceptable to the credit card industry or credit card users, a 3% uncertainty for medicine is far from the Six Sigma focus of accuracy levels of 99.99966%. There is an exponentially higher consequence of a fraudulent adrenaline injection restarting a heart after open heart surgery. While food fraud usually does not have a public health threat—and other than allergens, often never has an emergency, acute consequence—this is an example of data security considerations.

Review of Past Traceability Initiatives (RFID or Auto-identification): Cost $282 Million Per Company

The philosopher Georgy Santayana reportedly said, "Those who cannot remember the past are condemned to repeat it." For traceability the example may be a review of the RFID/Auto-ID initiatives from around the end of the dot-com rush in 2002; there were big statements of the benefits but few reports of the actual realized benefits. As with current interoperable enhanced traceability—essentially a more recent version of the same thing—the RFID/Auto-ID concepts were very promising.

- *RFID* is a *radio-frequency identification* which is a way that computers identify a package by sending radio waves to a label that has an antenna loaded with a code.
- *Auto-ID* is an *automatic identification* which is the ability to determine a product identity without an active process.
- *Non-line-of-sight* refers to the ability to identify a package or label without being able to actually physically "see" the label. For example, a label could be read on a package that is in the middle of a pallet, covered in an overwrap, or in a bag or shopping cart.

A consulting report that was published in the RFID Journal estimated "the theoretical retailer would gain approximately $78 million from increased sales and labor savings across all 800 stores by implementing the Auto-ID Center's technology for tracking cases. It could achieve benefits of nearly $150 million from tracking individual units" (RFID Journal 2002). These were reportedly "used moderately to conservative numbers when assessing the benefits that could accrue from such a system" (RFID Journal 2002).

Those benefits would require an investment of

> "$465,000 to track cases at the first store and an average of $62,000 per store for the entire system and $827,000 for the first distribution center and $353,000 per center for the entire system. That's an investment of $282 million for all 800 stores (RFID Journal 2002)."

The benefits were reported as "reduce labor costs, improve accuracy and boost throughput" (RFID Journal 2002).

That's a lot of labor, a lot of capital invested for on-hand inventory, and an assumption of very high costs of inaccurate stock picking. There were no specific details on how the benefits would be received whether reduced carrying costs of inventory on hand, reduction of lost or stolen goods, fewer rush delivery charges, opportunity cost benefits of reducing lost sales due to stock-outs, or others.

The 2002 article ended with "When will that happen? We don't know. The technology is still being worked through"(RFID Journal 2002). As of 2018, there did not seem to be any published specific results or case studies based on real projects.

Thus, while there was very high confidence the financial benefits when it came down to predicting how soon the benefits would be expected, the public statements were very cautious—the statements emphasized the technology was not ready for implementation and was still being developed.

Shifting to focus a bit on the underlying assumptions, from a basic ROI set of questions:

- **Cost**: A $282 million initial investment and the annual upkeep are undefined but could be 5% or $14 million per year. For the sake of argument, possibly use 1% or $2.8 million.
- **Return on investment**: Not revenue but decreased costs. So the benefit is not increased sales or increased valuation but the reduction in losses of $228 million (coincidence or not, this is very close to their estimated cost of implementation).
- **Time until return is realized**: Possibly 1 year after the system is fully functioning (the $282 million cost offset by the $228 million savings) and then at least 6 months for the benefits to be fully realized (e.g., actually experiencing the reduced costs of laid-off staff, losses avoided, inventory reduced, etc.). Note that the report stated that the system was still being developed so there was an undetermined time until return would start.
- **Confidence in the rate of return**: Undefined and not mentioned in the proposal.
- **Rate of return (at 2 years after investment)**: 0.4 ($228M–$128M/$228M) or about 2.5 years to break even on the investment. This is after the 2-year ramp-up.
- **Rate of return (at the start of full investment)**: So add 2+ years to the 2.5 year ROI until the project value is realized.
- **BATNA (best alternative to a negotiated agreement), the value of spending the funds elsewhere**: Undefined. The value of this individual project is not judged in and of itself (e.g., spend the money or not) since there are other uses for the funds (e.g., what is the best return on the investment across the entire enterprise). Due to the lack of details or specificity, the systems were not ready for an actual financial investment, so the current BATNA is the investment of time and energy thinking about the project.

So, from the data provided here, the ideal situation seems to be to listen and be a "fast follower."

Summary of CA-SB1476 (and then Why It Didn't Get Implemented)

Published by the California State Board of Pharmacy is a report on "Background and Summary of the California ePedigree Law." From that report that appears to be published in December 2017, several key sections are presented:

- "Problem: there is an increasing prevalence of counterfeit prescription drugs showing up in the US, intermingled [co-mingled] with the legitimate drug supply. Counterfeit prescription drugs are a worldwide problem, reaching as high as 30 percent of the supply in some countries. The World Health Organization estimates that in developed countries, counterfeit drugs are less than 1 percent of the market."
- "To put this in perspective: 3.4 billion prescriptions were dispensed in the US in 2006. If 1 percent of this supply is counterfeit, this would mean that perhaps 34 million of these US prescriptions were filled with counterfeit medicine. In California, we have roughly 9 percent of the US prescription drug market, so this would indicate that perhaps 3 million prescriptions were filled and dispensed with counterfeit medicine in 2006."
- "In an attempt to prevent counterfeit medicine from entering the legitimate supply chain in California, in 2004 the state legislature passed anti-counterfeiting and anti-diversion legislation (SB 1307), including provisions pertaining to the licensure and qualifications of wholesalers, restrictions on furnishing, and the requirement of an electronic pedigree to accompany/validate drug distributions. Portions of the legislation were implemented in 2005 and 2006. In 2006, subsequent legislation (SB 1476) [or CA-SB-1476] sponsored by the board moved the implementation date for the electronic pedigree component until 2009; the same legislation also augmented and clarified portions of the electronic pedigree requirements."
- "Under current law, as of 1/1/2009, no wholesaler or pharmacy may sell, trade or transfer a prescription drug at wholesale without providing, and no wholesaler or pharmacy may acquire any prescription drug without receiving, a pedigree. The **pedigree** is a record in electronic form containing information regarding each transaction resulting in a change of ownership of the given prescription drug, including returns. The law specifies the particular data elements pertaining to the drug and to each of the ownership links in the chain of distribution that must be included in this record and requires that the pedigree track each drug at the smallest package or immediate container (saleable unit). To implement this unit-level tracking requirement in an interoperable electronic system, requirements include a unique identifier (serialization number) placed on the smallest container saleable to a pharmacy, by the pharmaceutical manufacturer. Likewise, the manufacturer will also initiate the pedigree and pass that pedigree with the initial distribution; thereafter, the electronic pedigree will at all times accompany that particular container, appended by each successive owner to document each change of ownership of that particular container."

- "Simply put, the goal is for any owner/possessor of a prescription drug located at a licensed wholesaler, repackager, reverse distributor, or pharmacy in California, upon request, to have and keep electronic records that show the lineage of the drug from the manufacturer through to the current point in the drug distribution channel (wholesaler, repackager, pharmacy). The electronic pedigree must contain specific information required by statute and must be made and passed in an 'interoperable electronic system,' an electronic track and trace system based on unique identification numbers (serialization) affixed at the point of manufacture."
- "The unique identifier or unique serialized number on each saleable container of prescription drugs will most likely be carried either on a 2-D barcode or an RFID chip placed on the saleable unit by the manufacturer. The California Legislature has not mandated these specific technologies, but they are the two methods that have been identified that could meet the requirements of the legislation. The number on the serialized container could then be utilized to access the specific electronic pedigree for that individual container of a prescription drug."
- "Industry participants have engaged in standards-setting work to develop industry standards necessary to interoperability and sharing of pedigree data and records. The primary standards-setting body for the industry that has been engaged in this work with industry participants has been EPCglobal, the same entity that developed the standards for the UPC barcode."

Requirements:

- "**Pedigree**: means a record, in electronic form containing information regarding each transaction resulting in a change of ownership of a given dangerous drug, from sale by a manufacturer, through acquisition and sale by one or more wholesalers, manufacturers, or pharmacies, until final sale to a pharmacy or other person furnishing, administering or dispensing the dangerous drugs. The pedigree shall be created and maintained in an interoperable electronic system, ensuring compatibility throughout all stages of distribution. (California Business and Professions Code section 4034(a))."
- "**Interoperability**: this is one of the augmentations to the legislation in 2006. With input from industry, we determined for this pedigree concept to work effectively, all parties at all levels of the supply chain needed to be able to access the pedigree information without having to purchase numerous types of hardware, software, and middleware to be able to read whatever format a particular manufacturer chooses for their electronic pedigree. This will discourage companies from developing their own incompatible proprietary systems of electronic pedigrees, preventing the proliferation of systems and making it complex to read the pedigree by entities downstream (e.g., wholesalers and pharmacies). In January 2007, EPCglobal ratified a document-based pedigree messaging standard. Nearing finalization is a second EPCglobal standard, the EPCIS standard. The EPCIS standard would also allow the creation or appending of a pedigree, combined with a data storage and management system. This should be completed in several months."

- "**Interoperable electronic system**: As used in this chapter means an electronic track and trace system for dangerous drugs that use a unique identification number, established at the point of manufacture, contained within a standardized nonproprietary data format and architecture, that is uniformly used by manufacturers, wholesalers, and pharmacies for the pedigree of a dangerous drug. (California Business and Professions Code section 4034(i))."
- "**Serialization at the unit level**: this is the key to being able to enter, for instance, a pharmacy or wholesaler, to distinguish one container of prescription drugs from another, and to access the pedigree for each individual container. In addition, as long as the original container is available, the entire history of ownership for that specific container may be accessed. Specifically: "The pedigree shall track each dangerous drug at the smallest package or immediate container distributed by the manufacturer, received and distributed by the wholesaler and received by the pharmacy or another person furnishing administering or dispensing the dangerous drug" (California Business and Professions Code section 4034(d))."
  - "With the California system, two containers of the same drug, same strength, same lot number, and same expiration date, can be differentiated from each other. They each may have traveled very different supply chain routes to arrive at the same location. Only with the California serialized product can you tell each change of ownership for each container. The California process allows regulators to determine the origin of a container and be much more likely to identify when or if a product has been tampered with or if a counterfeit product has entered the supply chain."
- "**Repackaging**: This must be tracked on a single pedigree tracing back to the original manufacturer. Specifically: 'a single pedigree shall include every change of ownership of a given dangerous drug from its initial manufacture through to its final transactions to a pharmacy or other person for furnishing, administering or dispensing the drug, regardless of repackaging or assignment of another National Drug Code (NDC) Directory number' (California Business and Professions Code section 4034(c))."
- **"Returns**: These must also be tracked on a single pedigree. 'Any return of a dangerous drug to a wholesaler or manufacturer shall be documented on the same pedigree as the transaction that resulted in the receipt of the drug by the party returning it' (California Business and Professions Code section 4034(e))."

"The pedigree must contain (data elements):

1) The **source** of the dangerous drug, including the name, federal manufacturer's registration number or a state license number as determined by the board, and principal address of the source.
2) The **trade or generic name** of the drug, the quantity of the dangerous drug, its dosage form, and strength, the date of the transaction, the sales invoice number, the container size, and the number of containers, the expiration dates, and the lot numbers.

3) The **business name**, address and the federal manufacturer's registration number or a state license number as determined by the board, of each owner of the dangerous drug, and the dangerous drug shipping information including the name and address of each person certifying delivery or receipt of the dangerous drug.
4) A **certification** under penalty of perjury from a responsible party of the source of the dangerous drug that the information contained in the pedigree is true and accurate."

California law also requires that pharmacies may not act as wholesalers, and "A pharmacy may furnish dangerous drugs only to the following:

1) A wholesaler owned or under common control by the wholesaler from whom the dangerous drug was acquired.
2) The pharmaceutical manufacturer from whom the dangerous drug was acquired.
3) A licensed wholesaler is acting as a reverse distributor.
4) Another pharmacy or wholesaler to alleviate a temporary shortage of a dangerous drug that could result in the denial of health care. A pharmacy furnishing dangerous drugs pursuant to this paragraph may only furnish a quantity sufficient to alleviate the temporary shortage.
5) A patient or to another pharmacy pursuant to a prescription or as otherwise authorized by law.
6) A health care provider that is not a pharmacy, but that is authorized to purchase dangerous drugs
7) To another pharmacy under common control." (California Business and Professions Code section 4126.5)

An important final set of considerations focuses on the compliance and implementation:

- "**Sanctions**: In addition to other possible sanctions for non-compliance with pedigree requirements up to and including civil or criminal prosecutions, the board may cite and fine $5000 per occurrence (each saleable unit) or take formal discipline. Wholesalers must post a $100,000 bond with the board as a condition of licensure, which provides a source to pay any fines assessed."
- "**Reporting to the board**: a manufacturer, wholesaler or pharmacy with reasonable cause to believe a prescription medicine in or having been in its possession is counterfeit or subject of a fraudulent transaction shall notify the California Board of Pharmacy in writing within 72 hours of obtaining knowledge (only for drugs sold or distributed through California)."
- "**Implementation Delay**: the board can delay these requirements until 1/1/2011 if it determines, consistent with its public protection mandate, that manufacturers or wholesalers require additional time to implement electronic technologies to track the distribution of dangerous drugs within the state."

In many previous anti-counterfeiting or enhanced traceability programs or efforts, there were key challenges that were either difficult to overcome or that were insurmountable. Often the same problems keep derailing projects since history

wasn't reviewed. For food fraud prevention, there are important lessons to be learned from previous related programs and efforts. These lessons can both provide insight on how challenges were overcome and if they were insurmountable then to figure out sooner rather than later of what *cannot* be done.

Sidebar: California's E-Pedigree Law Preempted by Federal Regulation
Due to concerns about the slow adoption of the US Prescription Drug Marketing Act of 1987 (PDMA), the State of California passed a drug electronic pedigree law (Public Law 100-293 1988). Before the California e-pedigree law could take effect, in November 2013, federal "Public Law 113-54" was signed (CA-SB-1476 2006; Public Law 113-54 2011; DCA 2013). Details of the federal law include (DCA 2013):

- "This law contains provisions for a national track and trace system for prescription medication. Included within this law are provisions that preempt California's e-pedigree requirements. These provisions are in addition to those in the California Business and Professions Code that also preempt California's provisions should federal legislation in this area be enacted."
- "The [California State Board of Pharmacy] board is required to post a message about the inactivation of California's e-pedigree provisions. This notice is provided below; it also will be published in the ***California Regulatory Notice Register*** and posted on our website. Also this year the board will sponsor legislation to repeal the e-pedigree provisions that are now inactive provisions in California law."
- "The board thanks to the many individuals from pharmaceutical supply chain companies, computer and technology firms, policymakers, the staff of the California delegation and the many others who worked with the board over the last 10 years to develop e-pedigree provisions and implement a system to strengthen the integrity of the US drug supply."
- "We especially thank the early adopters and those who worked on pilot projects to ensure California's provisions would be implemented by the coming deadlines. It was a large endeavor, and we trust that what was learned to 'get ready for California' will be transferable to the national system that is now under development. We are grateful to have played a role in this important area of public safety and health."

- "Public Notice: Pursuant to Business and Professions Code section 4034.1, which provides in pertinent part that '[upon] the effective date of the federal legislation. .. addressing pedigree or serialization measures for dangerous drugs, Sections 4034, 4163(c) – (g), 4163.1, 4163.2, 4163.4, and 4163.5 shall become inoperative,' and which requires that within

(continued)

> 90 days of the enactment of such legislation the board publish a notice regarding the invalidation of these statutes, the California State Board of Pharmacy is hereby publishing notice that federal legislation meeting the requirements of section 4034.1 has been enacted, and that Business and Professions Code sections 4034, 4163, 4163.1, 4163.2, 4163.4, and 4163.5 became inoperative as of November 27, 2013."
>
> Efficient application of supply chain management theories includes the consideration of laws and regulations as well as systems for traceability and transparency. As the supply chain management principles may be new for food scientists, the compliance and application requirements are even more novel. Food fraud prevention is a problem based on a complex fraud opportunity and efficient and effective countermeasures, and control systems must consider an interdisciplinary approach based on lessons learned from previous efforts.

Conclusion

This chapter covered a follow-up on the previous chapter on supply chain management fundamentals with applications such as laws, regulations, standards, and certifications as well as traceability and transparency. The fraud opportunity is complex and based on issues that are created by a web of interactions and gaps. *The first conclusion is* that there are wide ranges of applicable laws, regulations, standards, and certifications. Earlier food industry efforts can add value to understand the current needs as well as a range of activities by other industries. It should be expected that others—either within the food or in other industries—have pursued protecting the supply chain. It should also be assumed that there are many lessons learned by very smart people who worked very intelligently to try to address very similar questions. There is a saying, "fraud prevention activities are twice as complex and complicated as you think it is and you know half as much as you think you know." *The second conclusion is* that traceability is complex and very specific needs should be the first focus of the project. "More" traceability is good, of course, but the exact value is undefined without an explanation of exactly how it addresses very specific problems. For example, regardless of the low-cost or easy, quick implementation, the new technology could be addressing a problem that is *not* above the risk tolerance. Also, it should be assumed that there are many very complex aspects of the system that could reduce the value of the result or even that could be a mission-critical issue that negates all value. *The final conclusion is* that the overall focus is on the transparency of the supply chain, transactions, and supply chain partners. With more transparency, there is a greater awareness of where the gaps or fraud opportunities occur and more specific insight on where and how suspicious product may be entering the supply chain. With more transparency, the fraud opportunity is reduced.

Appendix: WIIFM Chapter on Supply Chain Management Application

This "What's In It For Me" (WIFFM) section explains why this chapter is important to you.

Business functional group	Application of this chapter
WIIFM	There are a range of SCM systems and processes that increase transparency and traceability which reduce the fraud opportunity
Quality team	This application will tighten the control of inbound products and ingredients with respect to the fraud opportunity
Auditors	There will be some SCM-focused activities related to proof of product and ingredient authenticity as well as general transparency
Management	Suppliers need additional scrutiny which may seem like a lot of new overhead and controls, but that will actually *increase* purchasing flexibility to buy from a *wider* range of low-price suppliers
Corp. decision-makers	The purchasing group needs to support SCM assessments and controls to *increase* the buyer flexibility while operating under your risk tolerance

Appendix: Study Questions

This section includes study questions based on the Key Learning Objectives in this chapter.

1. Discussion Question
   (a) What is the role of "supply chain management" in FF prevention?
   (b) How does traceability increase supply chain transparency and reduce the fraud opportunity?
   (c) What are the attributes of traceability systems that were inefficient or that did not realize their ultimate potential?
2. Key Learning Objective 1
   (a) What are ISO and ISO 9000?
   (b) Why is thorough and reliable traceability difficult to manage and expected to be a "given"?
   (c) What is the role of a brand protection manager in FF prevention?
3. Key Learning Objective 2
   (a) Regarding traceability, what is "pedigree"?
   (b) What is "track" versus "trace" and why is there a need for both?
   (c) What are "inherent risks" of enhanced traceability systems?

4. Key Learning Objective 3
   (a) What is the "PDMA"?
   (b) What challenges hindered industry-wide—or overarching regulatory—requirements for e-traceability efforts?
   (c) What are some lessons learned from RFID initiatives?

References

Anthony, S. D. (2012). First mover or fast follower? Harvard Busines Review Online, Innovation, June 14, 2012, URL: https://hbr.org/2012/06/first-mover-or-fast-follower

Arway, A. G. (2016). *Supply chain security: A comprehensive approach*. Boca Raton, Florida: CRC Press.

Bazerman, M. H. (2001). Consumer research for consumers. *Journal of Consumer Research, 27*(4), 499–504.

Bix, L., Clarke, R., Lockhart, H., Twede, D., & Spink, J. (2007). Global data standards in the healthcare supply chain: The Business Case, prepared for The GS1 Healthcare Users Group (HUG). East Lansing, Michigan, Michigan State University, School of Packaging, May 30, 2007.

Bowersox, D. J., Closs, D. J., & Cooper, M. B. (2002). *Supply chain logistics management*. New York: McGraw-Hill.

BRIDGE. (2007). Building Radio frequency IDentification for the Global Environment (BRIDGE), Pharma traceability pilot, problem analysis, authors: John Jenkins Associates and WP6 partners, 11 July 2007, This work has been partly funded by the European Commission contract No: IST-2005-033546, Disclaimer: This document results from work being done in the framework of the BRIDGE project. It does not represent an official deliverable formally approved by the European Commission.

CA-SB-1476. (2006). California State Bill SB-1476, Figueroa Professions and vocations (AKA Drug Pedigree).

CSBP, California State Board of Pharmacy. (2007). Background and Summary of the California ePedigree Law, December 2007, URL: http://www.pharmacy.ca.gov/laws_regs/e_pedigree_laws_summary.pdf

CSBP, California State Board of Pharmacy. (2012). California's E-Pedigree Law, Supply Chain Integrity Workshop, U.S. Pharmacopeia May 22–23, 2012.

CSBP, California State Board of Pharmacy. (2013). California's E-Pedigree Law Preempted, November 27, 2013, URL: https://www.pharmacy.ca.gov/laws_regs/e_pedigree_law_preempted.shtml

DCA, California State Department of Consumer Affairs. (2013). California's E-Pedigree Law Preempted, November 27, 2013, https://www.pharmacy.ca.gov/laws_regs/e_pedigree_law_preempted.shtml

Dietrich, E., Puskar, E., Grace, A., Allen, M. A., & Schmitt, G. (2006). Considering RFID for use in the fight against counterfeiting. Emerging technology overview, Presented by the CACP's Technology Task Force, Coalition Against Counterfeiting and Piracy (CACP), U.S. Chamber of Commerce.

GS1, Global Standards 1. (2007). The GS1 Traceability Standard: What you need to know, January 2007.

GS1, Global Standards 1. (2018a). Global Trade Item Number (GTIN), URL: https://www.gs1.org/standards/id-keys/gtin

GS1, Global Standards 1. (2018b). Home Page. from https://www.gs1.org/

HDMA, Healthcare Foundation. (2004). Adopting EPC in Healthcare: Cost & benefits, 2004 HDMA Healthcare Foundation Adopting EPC in Healthcre: Costs & benefits, Published By:, HDMA Healthcare Foundation, by A.T. Kearny.

IRS, US Internal Revenue Service. (2018). Tax-exempt status for your organization, Publication 557, (Rev. January 2018). Cat. No. 46573C. URL: https://www.irs.gov/pub/irs-pdf/p557.pdf

ISO, International Organization for Standardization. (2005). "ISO 22000 Food safety management systems -- Requirements for any organization in the food chain." 2012, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35466

ISO, International Organization for Standardization. (2017). Technical Committee 292 Security Management and Resilience, Work Group 04 Product Fraud Countermeasures and Controls, Home Page, URL: https://www.iso.org/committee/5259148.html

ISO, International Standards Organization. (2011). "ISO 12931 - Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods." 2012, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=52210

Makadok, R. (1998). Can first-mover and early-mover advantages be sustained in an industry with low barriers to entry/imitation? *Strategic Management Journal, 19*(7), 683–696.

MSU-FFI, Food Fraud Initiaive. (2018). Blog series, food fraud initiative, Michigan State University, developed and presented by John Spink, URL: www.FoodFraud.msu.edu/Blog/

MSU FFI, Michigan State University Food Fraud Initiative. (2017). The role of enterprise risk management in food fraud prevention, MSU Food Fraud Initiative Report (FFIR), Funded by an anonymous donor, URL: http://foodfraud.msu.edu/wp-content/uploads/2017/03/FFI-Backgrounder-the-role-of-ERM-in-Food-Fraud-prevention-v50.pdf, URL Video: https://youtu.be/Cg8T9C8nURs

Porter, M. E. (1985). Technology and competitive advantage. *Journal of Business Strategy, 5*(3), 60–78.

Public Law 100-293. (1988). 100th Congress, An Act to amend the Federal Food, Drug, and Cosmetic Act to ban the reimportation of drugs produced in the United States, to place restrictions on the distribution of drug samples, to ban certain resales of drugs by hospitals and other health care entities, and for other purposes; Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled; SHORT TITLE.—This Act may be cited as the "Prescription Drug Marketing Act of 1987" (PDMA), URL: https://www.govinfo.gov/content/pkg/STATUTE-102/pdf/STATUTE-102-Pg95.pdf

Public Law 113-54. (2011). 113th Congress, An Act to amend the Federal Food, Drug, and Cosmetic Act with respect to human drug compounding and drug supply chain security, and for other purposes. <<NOTE: Nov. 27, 2013 - [H.R. 3204], Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, <<NOTE: Drug Quality and Security Act. 21 USC 301 note.>> SECTION 1. SHORT TITLE - This Act may be cited as the "Drug Quality and Security Act". URL: https://www.govinfo.gov/content/pkg/PLAW-113publ54/html/PLAW-113publ54.htm

RFID Journal. (2002). Auto-ID Center makes its case: White papers say a retailer with 800 stores could save $150 million per year from tracking individual items, September 5, 2002, URL: https://www.rfidjournal.com/articles/view?64

Spink, J. (2014). Food fraud prevention overview, Introducing the Food Fraud Prevention Cycle (FFPC)/ Food fraud prevention system, GFSI China Focus Day 2014, Beijing.

Spink, J., Zhang, G., Chen, W., & Speier-Pero, C. (2019). Introducing the food fraud prevention cycle (FFPC): A dynamic information management and strategic roadmap. *Food Control, 105*, 233–241.

Voss, M. D., Closs, D. J., Calantone, R. J., Helferich, O. K., & Speier-Pero, C. (2009). The role of security in the food supplier selection decision. *Journal of Business Logistics, 30*(1), 127.