CHAPTER 1.5

Illicit Trade, Supply Chain Integrity, and Technology

JUSTIN PICARD
Advanced Track & Trace

CARLOS A. ALVARENGA
Accenture

When did we start worrying about the origin of products we consume? Ethical, safety, and environmental concerns about products may seem to be a recent development—one that coincides with the acceleration of globalization. Yet a bit more than two hundred years ago, during the Age of Enlightenment, contemporaries of Voltaire were shocked to learn how brutally supply chains of the time often operated: “it is at this price that you eat sugar in Europe,” says the maimed slave to Voltaire’s Candide. Receding further, one finds the famous German Law on Beer Purity—restricting the allowed ingredients in the production of beer to water, barley, and hops—which dates from 1516 and is still in existence today. Yet our interest in product authenticity is probably even older: in ancient Rome, for example, fraudulent wine was common and seals were faked to pass lower-grade Gallic wine off as more costly Roman wine.

SUPPLY CHAIN INTEGRITY IS BECOMING A PRIMARY CONCERN

With the development of mass production techniques during the Industrial Age, this interest in provenance seems to have been put on hold for the better part of the last century. The accompanying development of branding allowed consumers to differentiate products that were generally similar, and made them comfortable and familiar with essentially anonymous goods. Today we talk of “product identity,” but for a while consumers nearly forgot that things do, in fact, have an origin. And why would consumers have bothered to worry about such things? In the pre-Internet era, brands could essentially master the message that was sent to customers, and the essence of that message was: “Trust me.” And for this trusted relationship, whether real or perceived, customers were and are still willing to pay a premium.

Thus for many decades the complexity and opacity of global supply chains made it very easy for some agents to hide, and for others to ignore, a wide array of illegal or unethical activities. This is a state that global markets can no longer sustain. Because supply chains have become an integral part of many a corporate strategy, supply chain integrity is no longer a marginal concern in the current legal, social, and business environment. Shareholders, consumers, civil society, and government have growing expectations that company executives be knowledgeable and accountable for what is happening in their extended supply chains. This goal, as every global brand manager knows in 2012, is much easier said than done.

Today, for any business that manufactures or sells globally, part of the usual price of success is becoming a magnet for counterfeiters; another part is the risk that counterfeits will infiltrate legitimate supply chains. The complexity and interconnectivity of supply chains mean that it is often very difficult to know what is going on beyond first-tier suppliers. Nonetheless, in the public’s mind, a global company is increasingly expected to ensure that every one of its suppliers respects labor rights and safety standards, uses environmentally friendly practices, and provides safe and reliable components and raw materials. But the brands themselves are not the only ones with issues. Shipping and logistics companies may not consider themselves responsible for the illegal acts of producers and importers, yet they are increasingly held accountable in cases of fraud or illegal transshipment. And although retailers have limited abilities to monitor the origin of all of their incoming goods—and thus to guarantee their customers genuine, safe, and ethically produced goods—their reputation is at stake each time the quality of products is compromised by one of their suppliers.

Supply chain integrity is increasingly at the top of supply chain managers' principal concerns. For example, in 2008 a PricewaterhouseCoopers study surveyed 59 global consumer and retail companies, and found that large brand-owners were particularly sensitive to both the reputational and operational risks of supply chains. Seventy-eight percent of respondents cited product safety as the most significant threat to their business; this was followed by concerns about business ethics including bribery, corruption and money laundering (61 percent); working conditions (59 percent); intellectual property (58 percent); broader human rights and community development issues (53 percent); carbon footprint (41 percent); local economic development and local sourcing (39 percent); and, last, broader environmental impact of product (34 percent).

As if product integrity were not challenge enough, the events of 9/11 had a global effect on supply chain security, and businesses had to integrate a whole set of new requirements related to cargo security and inspections. However, as extensive as these efforts were, they often ignored a major, and growing, concern: the origin and integrity of the product itself. For example, according to the International Organization for Standardization (ISO)'s specification for security management systems for the supply chain, "a supply chain is secure when it can resist, fend off, or withstand unauthorized acts that are designed to cause intentional harm or damage"—a definition that overlooks product origin and integrity.[1]

In the meantime, the complexity of supply chains has increased at the pace of globalization. Furthermore, the skills of counterfeiters, and those who would embed malicious code or technologies in otherwise safe products, have grown at the speed of technological change. These new priorities were recognized in the *United States National Strategy for Global Supply Chain Security,* unveiled at Davos in early 2012 by the US Secretary of Homeland Security Janet Napolitano. As stated in the *Strategy,* the number one goal will be to promote the efficient and secure movement of goods, and this will be achieved by "enhancing the integrity of goods as they move through the global supply chain."[2]

ILLICIT TRADE IN GLOBAL SUPPLY CHAINS

Illicit activities are, by nature, hard to monitor. They are often designed by perpetrators to avoid detection, and victims do not necessarily have an interest in reporting them. Yet many of these illicit activities could be detected and stopped before they cause significant harm, but they continue because of negligence or lack of rigorous protocols for controlling quality and provenance.

Illicit trade is typically associated with organized crime, or with seemingly legitimate actors who use the cover of a legitimate business to deliberately perpetrate a profit-based crime. Quite often, however, illicit trade involves multiple independent actors who do not necessarily work cohesively. Moreover, its harmful effects are the consequence not only of one crime, but of a sequence of fraudulent activities or acts of criminal negligence. For example, in 2007 the government of Panama unknowingly used Diethylene Glycol falsely labeled as Glycerine to make 260,000 bottles of cough syrup. The origin of the fake chemicals was traced from Panama through trading companies in Spain to a source near the Yangtze Delta in China.[3] The counterfeit glycerin passed through three trading companies on three continents, yet not one of them tested the syrup to confirm what was on the label. Along the way, a certificate falsely attesting to the purity of the shipment was repeatedly altered, eliminating the name of the manufacturer and previous owner. The result of this series of acts of negligence and falsification is dramatic: 100 people died in Panama from ingesting the deadly cough syrup.

Below are a few indicators of the scale at which supply chains are tampered with:

- The number of counterfeit incidents being detected in the US defense and industrial supply chain rose from 3,868 in 2005 to 9,356 incidents in 2008. This rise was facilitated by "demonstrated weaknesses in inventory management, procurement procedures, recordkeeping, reporting practices, inspection and testing protocols, and communication within and across all industry and government organizations."[4]
- The medication supply chain of lower- to middle-income countries appears to be corrupted to a frightening level. According to various studies, including a collaborative investigation of the World Health Organization and INTERPOL,[5] 50 percent of medications for malaria and 10 percent for tuberculosis are fake, and an argument can be made that these would kill approximately 700,000 persons per year.[6]
- A worldwide analysis of illegal and unreported fishing finds that current illegal and unreported fishing losses worldwide are between $10 billion and $23.5 billion annually (mean value of $16.75 billion, or 20.55 percent of declared import value), representing between 11 and 26 million tons.[7] Meanwhile, tests in stores and restaurants showed that fish was mislabeled 50 percent of the time.[8]
- Bottle refilling of wine, spirits, and food containers is a pervasive problem in many countries, and in the Far East it has become a big business.[9] There is a second market of empty spirit bottles, and some makers of spirits have had to launch costly

> consignment services to recover empty bottles while competing with counterfeiters on pricing. And, in a rather amusing twist, authentic empty bottles of luxury wine are fetching such high prices that even wine counterfeiters are sometimes cheated by the resellers of these empty bottles, who are supplying them with counterfeit bottles. One knows that supply chain integrity has become a concern for everyone when even counterfeiters get counterfeited.

In developed markets, supply chain integrity might still be seen—sometimes wrongly—as a manageable issue of risk and compliance. However, in high-growth emerging markets, tampered supply chains are a daily reality. As consumers become increasingly aware that the high level of corruption in emerging markets puts their health and safety at risk, they will expect manufacturers and retailers to be accountable for what they sell.

Incentives for illicit trade will continue to increase. Although the production of goods continues to be commoditized, there will be a continuous switch toward industries and markets that capture higher profit margins. High margins are captured through innovation, brand development, and ethical business practices. Although, in most cases, consumers cannot or do not make out the difference between products and their lower-end substitute, they still care enormously about origin. Many aspects of provenance are not visible in the finished product and provide free-riding opportunities for infringing parties.

THE REGULATORY BURDEN AND THE COMPLEXITIES OF COMPLIANCE

It is likely that terrorist attacks that either use or aim at global supply chains would bring disruption on a large scale. The illicit trading of weapons of mass destruction through a legitimate distribution channel—not to mention their ability to destroy critical infrastructure, such as a major port of entry—would probably force the temporary freeze and long-term reevaluation of security and monitoring processes in the global supply chain. But a subtler risk is that one major catastrophic event would engender fears that “global supply chains are out of control”—a reaction that would lead to sudden changes in regulations, which would place an increased burden on several industries. The Consumer Product Safety Improvement Act mentioned above is a US law that was passed hastily in the wake of several high-profile recalls in 2007 and 2008 of toys manufactured in China. If the public realizes that it is as exposed to threats coming from poorly monitored global supply chains as it was exposed to terrorist attacks on planes before 9/11, authorities might overreact by taking security measures akin to those that slowed down the flow of people through airport security following the terrorist attacks.

In many industries, growing consumer expectations over provenance are being translated into a dramatic increase in international regulatory enforcement actions. Furthermore, the lack of harmonization at the international level adds to the challenge that executives face in managing their global supply chains. For example, the California Transparency in Supply Chain Act, which was signed into law in 2010, requires disclosures on corporate efforts to eliminate slavery and human trafficking. The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 contains broad-reaching transparency provisions for oil, gas, mining, and other extractive industry companies. The Consumer Product Safety Improvement Act of 2008 imposes a variety of requirements on child-related products.

Even when manufacturers can hardly be suspected of complicity in illicit activities—they have no incentive to be complicit, and in fact curtailing illicit trade would be to their advantage—regulations can be far reaching. In July 2011, for example, the European Union adopted a directive intended to prevent falsified medicines from entering the legal supply chain. From early 2013, EU Member States will have to mandate obligatory features on the outer packaging of medicines to demonstrate that they are authentic, to strengthen requirements for the inspection of the manufacturers of pharmaceutical ingredient, and to oblige manufacturers and distributors to report any suspicion of falsified medicines.[10]

Although regulations are expanding at the national level, little is done to harmonize these at the international level. The official World Trade Organization position is that, although it is concerned with licit trade, illicit trade does not fall under its mandate. The topic is indeed sensitive, as different countries can have different understanding of what constitutes “illicit trade,” and may have different interests at stake. Despite all its efforts, the World Health Organization has not yet succeeded in developing a definition of *falsified medicine* (the term *counterfeit* itself is avoided as being a subject of controversy) that is acceptable to all its members.

This ambiguity at the international level generates two concerns. For multinational corporations, having to deal with different regulations as well as different sets of standards in each country generates costs, complexity, and uncertainty. And suppliers from developing countries are worried that ever-growing regulations that are in place ostensibly to curb trade in illicit products may increase their cost of compliance, alter the conditions of competition to their disadvantage, and in effect act as protectionist barriers to international trade.

TOWARD THE TRANSPARENT SUPPLY CHAIN

Engaged consumers, nongovernmental organizations, and activists have little concern for the subtleties of international policymaking or for the complexities of compliance. They have strong feelings of right and the wrong, and generally adhere to the principle that “if a party is not part of the solution, then it is part of the problem.” Many activists believe that companies that do not proactively address the environmental and social practices of suppliers at all tiers of their supply chain deserve to be “named and shamed,” and eventually boycotted, if they are within reach of consumers. As the speed and fluidity of information increases thanks to instant communication and social media, global companies will become increasingly vulnerable to these reputational risks.

Since the supply chain is often part of a company's competitive model, *transparency* is not necessarily a term that has a positive connotation for supply chain managers. Transparency can be associated with the reverse engineering techniques used to gain insights into a competitor's manufacturing process and profit margin, and which are now part of the tactics of nongovernmental organizations to determine whether suppliers with poor environmental or social records are involved. Whether they like it or not, companies will have to come to grips with transparency and accept that, whatever their marketing budget, they cannot fully control the message delivered to their customers unless it is harmonized with the product. If a company does not make transparent information available to their customers, others will take care of it. For example, GoodGuide provides a mobile phone application that allows consumers to "shop their values" by scanning product barcodes in order to get information on a product's health, environmental, and social impacts. If it turns out that the washing powder a consumer is about to buy has a low environmental score, GoodGuide will propose a more environmentally friendly brand as an alternative. In the same way that consumers can bypass a brand with GoodGuide, they can bypass retailers with SnapShop, a mobile application that scans a barcode to determine which offline or online retailer offers a better deal. Understandably, some businesses may feel they more have to lose than to gain with transparency.

In the fight against illicit trade, technology is a double-edged sword. For years, anti-fraud experts, as well as enforcement authorities, have repeated warnings that new technologies provide an edge to criminals. New technologies allow criminals to encrypt their communications, to operate from countries beyond the reach of law enforcement and reach a mass of anonymous consumers through the Internet, or to hack the protections developed to make counterfeiting difficult. In a session on cybercrime held in Davos earlier this year, Moisés Naím summed up this advantage by saying that "criminals move at the speed of Internet and countries move at the speed of democracy—that's the discrepancy."[11]

Many illicit activities take place because their perpetrators believe that they will remain unnoticed, or that there will not be enough evidence to demonstrate their responsibility. In other words, the rewards are high and the risks of getting caught and punished are low. However, there are two reasons why digital technologies, as they become more pervasive, can make the corruption of supply chains increasingly difficult. First, the development of product-tracking technologies, and their convergence with mobile communication technologies, is allowing an increasingly large number of parties to obtain reliable item-level information on provenance and to securely discern the licit from the illicit. Second, as processes in a supply chain get digitally recorded and managed with the proper data granularity, any licit or illicit activity will leave digital footprints that can be made nearly impossible to tamper with or erase.

PRODUCT-TRACKING AND AUTHENTICATION TECHNOLOGIES

The paradigm of security printing, where banknotes are produced behind closed walls and loaded with secret anti-counterfeiting technologies, does not adapt very well to the cost-constrained industrial world of outsourced production. Furthermore, traditional security features such as holograms and security inks can be easily imitated, as the technology and skills to reproduce them are now freely available on the market. However, new coding techniques are constantly developed to meet the needs of the corporate world and industrial products. For example, Coats Textiles in the United Kingdom has developed a "digital thread" with a security code embedded in the thread itself. It is invisible but can be scanned so it can be used to verify the integrity of clothing, parachutes, and so on—basically anything made from fabric. Invisible taggants, whether chemical or biological, can be inserted into a variety of materials or liquids. Spectral techniques have been developed to increase information capacity, allowing sources of product diversion to be identified. Invisible laser-etched code inside a supplier's manufacturing machines can verify the integrity of source down to the machine level.

There are now technology solutions for any type of product. Luxury goods such as high-end watches can be assigned a Smartcard, and can be authenticated instantly through the Internet via a Smartcard reader that is provided to customers. For fast-moving consumer goods, which can afford only a very low per-item protection cost, small digital graphics can be inserted into the packaging during the production process, and printed with standard industrial printers. One such type of secure graphic, called STAMPS (for "Secure Tracking and Authentication through Matrix Printing and Scanning"), is mathematically impossible to copy and can be authenticated through an image capture with a mobile phone.

If coding beforehand is not possible, alternative techniques can be used to check the product's characteristics. For example, Raman spectroscopic readers can verify whether the spectral profile of a medication or wine matches a reference profile. And while radio-frequency identification (RFID) tags are currently undergoing trials in Malaysian and Brazilian forests as a means of monitoring tree growth, tracking logged trees during transportation and finding and stopping illegal loggers,[12] Mother Nature provides us with free "DNA barcodes." DNA barcoding is a new scientific discipline that can be applied to detect illegal wildlife trade. Illegal logging can be detected from a piece of furniture, because wood from different species and also from different regions have distinct DNA barcodes. A project known as "The Barcode of Life" aims to produce a DNA barcode for every tree and grass species on Earth. Within a few years, the DNA barcode would allow the source of any sample to be identified.[13]

For the foreseeable future, the range of options for product tracking and authentication will continue to grow. But the large number of authentication solutions already on the market can increase the effort to determine which is the most appropriate to a given situation. This is why ISO standard 12931 on the performance criteria for authentication solutions, as well as other standards currently in preparation, can guide brand owners in the selection of the most appropriate technologies for their needs. Yet, however helpful these tools are, many of them remain accessible only to a small minority of authorized parties. The real breakthrough may actually come from open standards and technologies that may seem more basic, but are firmly established and accessible to the masses through their mobile phones.

THE CONVERGENCE OF PRODUCT AUTHENTICATION AND MOBILE COMMUNICATION TECHNOLOGIES

Consider the simple scratch codes that are typically found on lottery tickets. A handful of companies—such as mPedigree in Ghana, Sproxil in Nigeria, and PharmaSecure in India—are proposing to use these very codes as a simple solution to the scourge of counterfeit drugs in developing countries. As a consumer buys a drug, he or she can reveal the code, short message service (SMS) it to a toll free phone number, and receive feedback on its authenticity within seconds. As the codes are random and "verify once," they cannot be guessed or reused by counterfeiters. Similar 12-digit codes are used by the tobacco industry to address the problems of tax avoidance, smuggling, and counterfeiting, which cost governments an estimated $50 billion in lost taxes each year.

User convenience and consumer adoption are key to the success of any consumer-based anti-fraud system, and typing a code on a mobile phone or through an online service might in the end be slightly too inconvenient for integration into consumer habits. RFID chips automate the scanning process, and the idea of using them on products at the item level has been around for years. Although they are still too expensive for many product categories, the main limiting factor today is that only a small number of mobile phones are equipped with near field communication (NFC) readers. If, as expected—or at least rumored—the next generation of smart phones integrates NFC, placing RFID chips on higher-end products will start to become more common.

2D barcodes are high-capacity optical data carriers that might offer the right compromise between the low cost of implementation and the convenience of scanning. Although they were initially developed to help item identification and traceability in various industries, 2D barcodes are increasingly used for mobile marketing. There are now tens of different symbologies (i.e., methods to represent data), and although that could be a handicap for streamlining adoption, this large number indicates serious interest in these technologies. The most popular formats—the QR (for "Quick Response" code) and Data Matrix—are free to use and based on open ISO standards. Open source code for encoding and decoding the symbols is available, allowing any programmer to launch a mobile phone barcode decoding application. In the meantime, the optics and processing power of mobile phones have tremendously improved, and consumers have started to read those barcodes as they shop. When those codes contain a Web address, the decoding software automatically redirects the user to the Web page. If codes are serialized, item-level traceability can be pushed to the consumer who, in return, can provide feedback that is connected to a specific product.

2D barcodes and RFID cannot be forged as long as they use encryption or have a random part that is matched with a database. That is, a non-authorized party such as a counterfeiter cannot guess new valid codes. Yet these technologies have one fundamental weakness: there is nothing that prevents them from being copied. However, active monitoring can compensate for this weakness. Counterfeiters typically use one or a few codes and massively replicate them. Counterfeit codes therefore generate an abnormally high number of scans, and can be automatically or manually blacklisted. Once a counterfeit code is blacklisted, the authentication system becomes foolproof. Because retailers and consumers vastly outnumber the small investigation teams deployed by brand owners, they can potentially multiply the deterring effect of authentication technologies.

DIGITAL FOOTPRINTS

The convergence of mobile communication, product tracking, and authentication empowers a larger number of stakeholders to access relevant traceability information. Each time a product is checked, a feedback loop that enriches information flows and reinforces the system is created. However, the fact that a manufacturer adds a code or label to the product does not in itself guarantee that all the product-claimed attributes are respected. How is reliable traceability information created in the first place?

On some goods, outbound logistics provenance is vital. This is typical of cold chains for vaccines and medical products, frozen food, and agricultural produce. Simple solutions involve placing time-temperature indicators that change color to signal the occurrence of a potentially damaging heat or freeze event, or the presence of food-borne pathogens. More sophisticated systems use RFID sensors to monitor or record temperature, geographical position, and other events—such as a container opening—at any point along global distribution channels. Such systems are now in use for fine wines, for example, since it was realized that all the effort put into wine making can be destroyed through a careless distribution system. Indeed, according to experts, 10 to 25 percent of the wines sold in America are damaged during transport because of their exposure to extreme temperatures.

With basic "Ok/Not Ok" monitoring systems, a food or product safety crisis can be prevented. But digital footprints have a deeper impact because they create conditions for continuous improvement and accountability, as each stakeholder in the supply chain receives objective feedback on his performance. Moreover, if the required transport conditions are not maintained, responsibilities can be unambiguously assigned.

The sources of legitimate product and illegitimate goods are often intermingled. For example, there are cases where a manufacturer produces two versions of its product: one destined for the legitimate supply chains and one, made during the "ghost shift," destined for illegal ones. The unlicensed version of the legitimate product is sold often at a higher margin. Yet if the problem comes from a supplier, legitimate quantities can be simply controlled by providing counterfeit-proof serialized labels that must be attached to the legitimate products, according to the ordered quantities.

Of course, dealing with a multi-tier supply network involves a different level of complexity. In this case, placing a simple tag on a component does not necessarily fix problems with suppliers, but it can be an enabler. The important thing is to fit technology into a process that records relevant traceability information, holds the supplier accountable, and makes successful fraud much more difficult because the coherence of the digital trail must be maintained. For example, if a tag is provided to the supplier and assigned to each supplied component, the quality control can be digitally recorded by reading the tag, thereby leaving a permanent trace. The very act of reading the tag can be made equivalent to a digital signature, testifying that, for instance, the supplier has respected a specific quality-control process.

CONCLUSION

The problem of supply chain integrity is an old one in society but a relatively new one in global supply chain management. Its importance has mounted because of the increasing global reach of brands and the lack of accountability in supply chains that operate in many parts of the world. Combined with the new supply chain security risks that use products as vehicles—such as malicious embedded software, bombs in ink cartridges—a new sub-discipline is needed within supply chain risk that might be called "chain of custody management" or "supply chain integrity management." Basically, the focus of this new aspect of supply chain risk management is to answer the four questions of product-level supply chain integrity:

1. 1. *Integrity of source*: Does this product come from where I think it did?
2. 2. *Integrity of content*: Is this product made the way I think it is?
3. 3. *Integrity of purpose*: Is this product going to do exactly what I think it will?
4. 4. *Integrity of channel*: Did this product travel the way I think it did?

In the end, the strategic shift is that information regarding the integrity of the product in the future will be provided not by the supply chain but by the product itself. Gone are the notions that counterfeiting and fraud on the "illegitimate" supply chain is a tolerable cost of doing business, and that there would be an impenetrable, well-controlled legitimate supply chain in which consumers are encouraged to make their purchases. In the future, a consumer will have to be able to trust a product coming from the back of a pickup truck in an unregulated nation with the same confidence as if he or she were taking it off the shelf of a reputable retailer. That may sound far-fetched, but there is now an ecosystem of tracking and communication technologies that has an incredible potential to provide more transparency of supply chains, easier access to information, richer and more granular traceability, enriched communication with consumers, and the ability throughout the supply chain to discern the licit from the illicit. The technology is here now. It just needs to be put to work.

NOTES

[1] ISO 28000:2007.

[2] whitehouse.gov 2012.

[3] Bogdanich and Hooker 2007.

[4] US Department of Commerce 2010.

[5] Newton et al. 2008.

[6] Harris et al. 2009.

[7] Agnew et al. 2009.

[8] Styles et al. 2011.

[9] Pierson 2012.

[10] European Parliament 2011.

[11] *The Times* 2012.

[12] Springwise.com 2011.

[13] Luntz 2011.

REFERENCES

Agnew, D.J., J. Pearce, G. Pramod, T. Peatman, R. Watson, et al. 2009. « Estimating the Worldwide Extent of Illegal Fishing. » *PLoS ONE 4* (2): e4570. Available at http://www.plosone.org/article/info:doi/10.1371/journal.pone.0004570.

Bogdanich, W. and J. Hooker. 2007. "From China to Panama: A Trail of Poisoned Medicine." May 6. *The New York Times.*

European Parliament. 2011. "DIRECTIVE 2011/62/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011." *Official Journal of the European Union* 1.7.2011. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:174:0074:0087:EN:PDF.

Harris, J., P. Stevens, and J. Morris. 2009. *Keeping It Real: Combating the Spread of Fake Drugs in Poor Countries.* International Policy Network. Available at http://www.policynetwork.net/sites/default/files/keeping_it_real_2009.pdf

ISO (International Organization for Standardization). 2007. *ISO 28000:2007.*

Luntz, S. 2011. "Forests Meet Forensics." *Australasian Science,* September. Available at http://www.australasianscience.com.au/article/issue-september-2011/forests-meet-forensics.html.

Newton, P. N., F. M. Fernández, A. Plançon, D. C. Mildenhall, M. D. Green, et al. 2008. « A Collaborative Epidemiological Investigation into the Criminal Fake Artesunate Trade in South East Asia. » *PLoS Med* 5 (2): e32. Available at http://www.plosmedicine.org/article/info:doi/10.1371/journal.pmed.0050032

Pierson, D. 2012. "Pricey Counterfeit Labels Proliferate as China Wine Market Booms." January 14. *Los Angeles Times.* Available at http://articles.latimes.com/2012/jan/14/business/la-fi-china-counterfeit-wine-20120115.

Springwise.com. 2011. "In Malaysia, RFID Used to Stop Illegal Logging." Eco & Sustainability, December 9. Available at http://www.springwise.com/eco_sustainability/malaysia-rfid-stop-illegal-logging/

Stiles, M. L., H. Lahr, W. Lahey, E. Shaftel, D. Bethel, J. Falls, and M. F. Hirshfield. 2011. *Bait and Switch: How Seafood Fraud Hurts our Oceans, our Wallets and our Health.* Washington DC: Oceana. Available at http://oceana.org/sites/default/files/reports/SeafoodFraudReport_041811.pdf

The Times. 2012. "Davos Live: EU Transaction Tax Is 'Madness'." Davos 2012, presentation, January 26. Available at http://www.thetimes.co.uk/tto/public/davos/article3299180.ece.

US Department of Commerce. 2010. *Defense Industrial Base Assessment: Counterfeit Electronics.* Washington DC: US Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation. Available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

whitehouse.gov. 2012. *National Strategy for Global Supply Chain Security,* January. Available at http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.