MITSloan
Management Review

Taming the Counterfeiting Epidemic

A multilayered approach is essential to effectively combat counterfeiting and unauthorized sales.

Robert Handfield
Anand Nair
Thomas Y. Choi

• Reprint #65107 • sloanreview.mit.edu

Taming the Counterfeiting Epidemic

Robert Handfield, Anand Nair, and Thomas Y. Choi

A multilayered approach is essential to effectively combat counterfeiting and unauthorized sales.

Neil Webb/theispot.com

Whether their leaders know it or not, many companies are losing significant revenue to counterfeiters and unscrupulous supply chain partners. Anyone perusing handbags at a street market knows how common it is to find fake products that look identical to the real thing but might not function the same way. In some cases, this can put consumers at risk: A pharmaceutical company, for instance, discovered counterfeit versions of its product on the black market that contained no active pharmaceutical ingredients. As well, a company's legitimate product may be diverted for unauthorized sales, as when a global electronics company discovered that distributors in its network, who had ordered components supposedly for customer repairs, were selling them on the gray market.

High-demand products in every industry are lucrative targets for fraudulent criminal activity. Unfortunately, counterfeit products are a problem that many companies do not want to acknowledge or raise to their boards or shareholders. Senior executives often try to explain away the problem, rationalizing that counterfeiters will always find a way to copy products or that piracy represents only a small percentage of sales and is not worth going after. That plays right into the hands of what counterfeiters want businesses to do: ignore them.

When companies do begin to quantify the level to which counterfeiters are affecting their bottom lines, they may attack the problem with piecemeal approaches to try to prevent it from growing. But that's not enough.

Our research suggests that successfully combating counterfeits requires the attention of a broad collection of organizational functions. It works best with a multilayered strategy encompassing diverse methods and engaging the entire organization and its partners.

We recommend that organizations tackle counterfeiting with a cohesive plan for identifying, containing, and preventing it. This comprehensive process means routinely keeping tabs on contract manufacturers and charting how products move through the supply chain. It includes scoping out what is for sale in consumer markets, deploying covert markings, reviewing warranty claims, educating customers, and partnering with key agencies and competitors.

Conventional Tactics Aren't Working

Companies that pay any attention to counterfeiting have traditionally relied on a brand security function to track down criminal activity. These teams often detect counterfeiting using tactics such as applying covert and overt markings on legitimate products, attaching RFID tags that track product locations, and using serialization combined with blockchain to create transaction records that are resistant to tampering. For example, barcodes compliant with the GS1 Global Traceability Standard are used to track COVID-19 vaccines. [1] For many organizations, though, these tactics are not enough.

Counterfeiting and illegal diversion of product remains pervasive: Our 2018 survey of 21 supply chain executives revealed that nearly half had an issue that was ongoing or had experienced an incident in the previous year. More than 70% said they'd had an incident in the previous five years. (See "The Research.") One executive told us that his company discovered that the equivalent of an entire factory's monthly production of its products was being sent into black markets, largely due to diversion from one of its own suppliers.

Counterfeiting has grown into a problem that the Organization for Economic Cooperation and Development says was worth $464 billion in 2019, or 2.5% of world trade. [2] It was once thought that counterfeiters went after only high-value or luxury items such as pharmaceuticals, designer handbags, or perfume. But now the marketplace is full of fake footwear, pesticides, cosmetics, toys, automotive parts, and medical equipment. Counterfeiters are targeting any industry and any product line where there is an easy profit to be made.

While companies may never completely eliminate bad actors from copying products or diverting goods from authorized channels, they can significantly reduce counterfeiters' market penetration and restore lost revenue. Successful approaches may involve cutting off counterfeiters' access to markets, eliminating their supply of unauthorized goods, or making a product more difficult to copy. Here, we'll go into detail on the three activities that a robust action plan comprises: identification, containment, and prevention.

Identification: Gain Insight Into the Extent and Nature of the Problem

Getting a baseline on the severity of the counterfeiting problem is a critical first step. As the size of the issue becomes clear, the potential return on investment in shutting it down also comes into view. This can help establish performance metrics for the anti-counterfeiting team that can be aligned with business objectives and outcomes. Examples of metrics include the dollar amount or percentage of revenue lost annually due to illegal product trade, total top-line revenues recovered (dollars that were previously unknowingly lost to counterfeit sales), and the number of confirmed incidents of illicit trade, counterfeiting, diversion, and tampering.

Create a cross-functional brand security team. Developing realistic measures of the current problem often requires an intensive investigation that involves applying market channel analyses that explore multiple sources of sales data and other information from both inside and outside the organization. To be effective, a brand security team should include participants from sales, marketing, operations, purchasing, logistics, finance, and accounting, as well as core brand security functions. Such teams are typically led by a global brand protection officer who in many cases has a law enforcement background and usually reports to the chief operating officer.

Examine internal and market data to flush out suspicious activity. Companies can struggle to find, much less measure, counterfeiting activity, given that clues are usually buried in data about sales, warranties, returns, and other product metrics. Unless someone is looking for it, unusual activity can easily go unnoticed.

A good first step is to start by looking at what's being sold online. E-commerce has emerged as a perfect channel to fuel the counterfeit goods industry. Consumers may unwittingly buy products from online retailers that don't verify the

source of the products on their platform and whether they are legitimate. Despite counterfeit sites being shut down regularly by Amazon (and, in China, Alibaba), operators trading in fake goods regularly open up again under a different name the next day. Amazon reported that it blocked 10 billion fake listings and destroyed 2 million counterfeit products in 2020 alone. [3]

Since e-commerce sites are frequently a counterfeiter's primary source of sales, companies can begin by investigating where their products — either genuine or fake — are being sold online. Looking for common attributes of counterfeiter websites can narrow down the pool of suspicious activity. For instance, a company might find four different sellers on Amazon offering an exact copy of its handbag, listing the same details and even photos. An indicator of potential counterfeiters might include spelling or grammatical errors, blurry photos, or other details that don't look quite right.

Another important data source is warranty returns. When a consumer sends a product back because it is defective (and counterfeits often are), detective work can track down where it was purchased and how. This can lead to the origin of market entry for counterfeit goods and a starting point to find their downstream source. A global medical products company we looked at hired a global brand protection officer who examined warranty and returns data, field service requests, and sales data. In his first 100 days, he found 1,000 confirmed incidents of illicit trade, counterfeiting, diversion, and tampering. This amounted to $1.4 billion — 2% of revenue — lost annually to illegal product trade.

Estimating counterfeit sales is a difficult but essential task: Companies must establish a baseline against which to gauge the effects of anti-counterfeit measures. Having an accurate understanding of the scope of the problem is a prerequisite for deciding how much to invest and what ROI to expect from anti-counterfeiting measures. In many cases, business decision makers are unaware of the extent to which their revenue and reputation are in jeopardy.

Map the supply and distribution chain. Many companies are surprised to learn that bad actors are active within their own supply chains. Overproduction, black-market sales, and unauthorized distribution are common sources of leakage that may result in a product, or copies of it, being sold through channels that a company knows nothing about. That's why an important early step is to identify the manufacturing and distribution channels through which the company's products travel.

The brand owner at a large global apparel company told us that he had heard through his distributor network that the brand was being sold in Mexico even though the company had no authorized retail presence there. To track where these products were coming from, the director hunted down bills of lading and shipping records for the ocean freight shipments that were going to Mexico. The paper trail showed that the goods were shipped from a port in Israel — by the same authorized manufacturer that was producing the company's branded product in the United States. The apparel company eventually tracked down the clothes, which were genuine products, made under the same specifications and from the same materials, but were being illicitly distributed outside of the contractual agreement between the parties. When the apparel company set up a global brand security function and mapped its entire supply network, it found that similar cases of product diversion were occurring all over the world.

Analyzing how much is being spent on raw materials in the upstream supply chains is a good place to start mapping a supply base. Procurement can reach out to the accounting team to track all third-party purchases being made on the company's behalf (a document generally known as a *spend analysis*). If a supplier is buying more raw materials and is operating at a higher production level than what the company is ordering, this is a telltale sign that the additional product may be moving into the black market. This requires full visibility into the supply chain, beyond just Tier 1 suppliers (which is increasingly important for other reasons, in particular to manage risk related to labor or environmental violations). Some suppliers may be reluctant to disclose their upstream suppliers for competitive reasons but can be reassured that the query is for security purposes and not an attempt to cut them out of the chain.

Containment: Limit the Problem's Spread

With a dedicated team in place, an initial sense of the problem's scope, and an understanding of the particular counterfeiting and diversion risks that it's most vulnerable to, a company can begin to manage the problem systematically in order to contain it.

Analyze product segments. One of the key tasks for the investigation team is segmenting products by channel, margin, volume, and risk of counterfeit activity. This ensures that the team's attention is being directed toward the most vulnerable market channels first.

In many cases, a current-state analysis of a company's supply and distribution processes helps reveal a common set of product segments that counterfeiters go after. In particular, our research found that product lines with high complexity based on the variety of finished products, level of finished-product customization, geographical span of suppliers, number of tiers in the supply chain, predictability of demand, and variation in manufacturing volumes. Examples of items in this category include aircraft and automotive replacement parts, toys, high-end apparel, branded pharmaceutical products, and consumer electronics. Counterfeiters are more likely to opportunistically target product segments characterized by a greater level of complexity and exploit this complexity to their advantage.

We interviewed executives at a biotech manufacturer who knew that counterfeit products were showing up in the market but did not know the source. The brand protection team started by segmenting products into those that were big targets for counterfeiters (in this case, high-margin items) and analyzing data to estimate the number of incidents per brand. The team — formed through a close collaboration among franchises, brand owners, and regional sales managers — then rolled out a plan to franchise partners and country business units. This established brand protection priorities by product line and provided a system to track customer-reported incidents by brand and conduct data reviews every six months.

At the same time, analysts began collecting market intelligence on supply chain vulnerabilities, including potential logistics disruptions and the threat of regulatory intervention, that posed significant risks for business plans and growth targets by region. Cumulatively, these efforts helped the manufacturer prioritize those businesses and regions where brand protection could best safeguard market revenue from sudden disruptions. In the process, the team identified a significant counterfeit and diversion activity affecting a blockbuster infusion drug that was putting many patients at risk. The company said it was able to eventually reduce the number of incidents from 100 per year to zero. This required persistent efforts to deduce the source of each incident through detailed analysis and the introduction of countermeasures — including sending a message to counterfeiters warning that they would be pursued, in hopes of convincing them to go look for an easier target.

This kind of analysis begins with identifying an initial clue and following the thread of activity. The initial problem may manifest itself as a minor issue such as a customer warranty problem, a dealer who seems to be ordering too many replacement parts, or a spate of customer returns on a particular brand of product. Any of these issues may be a hint that leads to a channel of counterfeiting activity.

Start with e-commerce sites, and reach out to customs and other authorities. A team of analysts should be hunting down in-the-open counterfeit operations on e-commerce sites on an ongoing basis and reporting them to the platform operator, such as Amazon, and to law enforcement. At the very least, this introduces more friction into some bad actors' businesses to slow them down.

Counterfeit products almost always have to cross borders and pass through transshipment points and customs inspections overseen by law enforcement entities. These are critical players in the supply chain, and organizations must think of them as partners in the battle against revenue loss and intellectual property theft. These relationships are particularly important in highly regulated environments, such as pharmaceuticals, food, aerospace, and automotive manufacturing, where counterfeit products can endanger their users.

An official with U.S. Customs and Border Protection (CBP) told us that it can be challenging to get brand owners to

understand the CBP's process and play their part in helping the agency fight the problem. "We are in the field, inspecting containers," he said. "If a CBP officer opens a container and sees something that looks suspicious, they will first look in our internal database of registered brands. If the officer doesn't see anything, there is nothing they can do." Registering brands with the CBP and U.S. Patent and Trademark Office is a critical step in containing counterfeiting.

Educate (and warn) customers. It is imperative that consumers are educated about the possibility and risks of buying fake goods. Companies should make customers aware, through brand marketing, that if they buy from an unverified online third-party seller, they bear the risk of not having the product covered by warranty — or, worse yet, having it fail with dire consequences. One company we know of began adding a statement on its Amazon website warning that products returned to it that were not licensed would not be under warranty. Companies should also emphasize to customers the importance of registering the product serial number for warranty purposes, which protects them if a legitimate product they've purchased turns out to be flawed or faulty. If a customer tries to register the serial number for a counterfeit product, it will show up as an error and alert the brand security team to a problem.

Prevention: Stop Future Counterfeit Ops Before They Start

Once an organization discovers how the spread of counterfeit products in its market channels works and has taken initial steps to contain the problem, it must continue to monitor criminal activity and establish strong preventive measures. There are important roles for numerous functions in the company to play at this stage.

Product packaging experts should explore digital tracing technology. Features in current tracing technologies offer positive product authentication, can indicate tampering, can increase the difficulty of replication, and permit product tracking and tracing. Secure markings — which use a variety of packaging, blockchain, and serial marking technologies — are one method for tracking products. Many industries are working with standards organizations like ASTM International or GS1 to develop common methods for verifying products. This can help avoid the problem where counterfeiters try to copy not just the product but the digital marking, too.

In the biotech example mentioned previously, the brand protection team worked with the business to identify covert and overt authentication capabilities, which created automatic alerts when counterfeit products were being sold through market channels. The team also created a comprehensive customer communication plan using web advertisements, targeted email and Twitter campaigns, and retailer alerts about the dangers of buying from unauthorized sources. The campaign created awareness in the company's sales partner network and set the stage to identify where new counterfeit sales were occurring.

Quality assurance should review data to track down instances of product problems and returns. QA can create triggers in its data collection processes that flag potential illegitimate activities. We know of a company that noticed an uptick in its product returns, discovered that the products were not legitimate, and tracked them down to the point of sale — which revealed the source of the counterfeiting.

Supply management should step up efforts to audit suppliers. It can be particularly fruitful to track overproduction by suppliers, as well as how they dispose of products that don't conform to quality standards — products that can end up moving through black market channels and thus avoiding trade compliance policies. One large apparel company began monitoring the inventory levels within its supplier's facilities and noticed that the supplier's inbound raw-material inventories were much greater than the volume of finished goods it was shipping to the company. This was an indication that product was being produced and sold elsewhere through other channels.

Logistics should map supply routes to document compliance on the part of transportation providers. This can help ensure chain of custody along global supply chains, particularly at handoff points such as ports, warehouses, and distribution centers. Companies with multitier distributor channels

should document every logistics handoff and conduct random audits to determine whether there are proper security personnel and locked gates at all distribution centers.

Human resources might want to consider monitoring employees who are dealing directly with targeted products. This may include conducting background checks, as well as increasing training to enhance staff awareness. If there is a high level of missing inventory or a sudden increase or drop in product sales, investigations may be required.

Aftermarket sales should track warranty claims and parts sales to identify product-quality problems. As with the quality assurance team, those at the front line of aftermarket sales are in a position to learn that products aren't performing as expected, which, again, may indicate that counterfeits are entering market channels. For example, a large retailer made the decision to limit its distribution channels and authorized resellers, recognizing the high potential for counterfeit products in these particular sales channels, especially e-commerce.

Counterfeiting and product diversion are not crimes that a single organization can combat. They require the diligence of brands, retailers, packaging companies, and logistics businesses. This is a rare instance where joining with competitors can yield important insights. Companies should consider joining a consortium and partnering with industry counterparts. Industry-specific groups include the Automotive Anti-Counterfeiting Council for vehicle manufacturers and Rx-360 for pharmaceutical companies. Members of React, a large anti-counterfeiting network, include Marvel Entertainment, Mattel, Pfizer, Philips, Prada, and Timberland.

Counterfeiting is also not just a private-sector supply chain problem. Labor and human rights advocates, consumer education agencies, customs agents, federal and state law enforcement agencies, local police, and consumers of counterfeit products all have an interest and role in ferreting out unauthorized activity. While counterfeiting and product diversion cannot be eliminated, dedicated efforts can curtail both significantly.

About the Authors

Robert Handfield (@robhandfield) is the Bank of America University Distinguished Professor of Supply Chain Management in the Poole College of Management at North Carolina State University. Anand Nair is a professor of supply chain and information management in the D'Amore-McKim School of Business at Northeastern University. Thomas Y. Choi is the AT&T Professor and a professor of supply chain management in the W.P. Carey School of Business at Arizona State University.

References

1. "GS1 Healthcare Reference Book 2021-2022: Stories of Successful Implementations of GS1 Standards," PDF file (Brussels: GS1 Healthcare, 2020), https://gs1ca.org.

2. "Global Trade in Fakes: A Worrying Threat," PDF file, (Paris: OECD Publishing and Illicit Trade, 2021), 9, www.oecd.org.

3. J. Pisani, "Amazon Blocked 10 Billion Listings in Counterfeit Crackdown," AP News, May 10, 2021, https://apnews.com.

The Research

- The authors conducted research into the state of counterfeiting from 2017 through early 2020. Funding was provided by CAPS Research, a joint venture of Arizona State University and the Institute for Supply Management.
- During the discovery phase, they ran an in-person workshop and attended the October 2017 annual strategic summit of the Center for Anti-Counterfeiting and Product Protection of Michigan State University.
- The authors conducted individual interviews with more than 20 subject-matter experts in 2017 and 2018.
- The authors also conducted in-depth surveys with 21 supply chain executives in June and August of 2018.

MITSloan Management Review

PDFs ■ Reprints ■ Permission to Copy ■ Back Issues