

THE

A B C S

OF BRAND PROTECTION
EBOOK



Table Of Contents:

Dark Arts: The Forms Counterfeiting Takes	3
Spotlight on Agrochemical	5
Different Features, Unique Purposes	7
Digital Solutions	9
Spotlight on Pharma	10
A Winding Path: Identifying and Implementing an Effective Brand Protection Program	11
Five Steps to Defining Risk of Product Compromise	11
How to Select a Brand Protection Partner	13
Spotlight on Fast Moving Consumer Goods	15
The Future of Brand Protection	16



The negative impact of counterfeiting and piracy is projected to drain US \$4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk by 2022.¹

ARE YOU READY? YOU NEED TO BE.

Whether you're a seller or a buyer, chances are you've encountered counterfeit products. In fact, it's estimated that more than 80 percent² of all global consumers have unwittingly purchased falsified products.

With the increasing volume of counterfeit goods trafficked across the globe, and seeping into your supply chain, a brand protection program is more essential than ever to shield what matters most to your business – customers, brand, and revenue.

This growing counterfeiting epidemic extends across a multitude of industries – food and beverage, pharmaceutical, health and beauty, apparel, and a host of other consumer and commercial products. The effects translate into financial losses for brand owners, and more importantly, added risks to consumer health and safety. Falsified products manufactured without regard for required ingredients, quality control or government oversight, imperil consumer safety, and lead to a potential lack of confidence in a once-trusted brand.

Many organizations have firm defenses in place, with policies and dedicated infrastructure to combat product fraud. Usually, brand owners team with a trusted third-party technology and solution provider. In fact, the global authentication and brand protection market is projected to reach US \$7.66 billion by 2026³. In the pharmaceutical industry alone, counterfeiting was estimated to exceed US \$200 billion in 2019, according to the World Health

Organization (WHO). In fact, experts say that more than 30 percent of all drugs sold in developing countries are falsified, putting millions of lives at risk each year. Industries where goods are critical to human health have been on the front line of the struggle, while others have been slower to adopt brand protection solutions – at their own peril.

Consider this: The global economic value of counterfeiting and piracy could reach US \$2.3 trillion by 2022.⁴

While early adopters have seen a vast improvement in the detection and reduction of counterfeit goods, companies in just about all industries are facing intensifying counterfeit issues as distribution goes global and visibility into the supply chain is obscured. The good news is that today's anti-counterfeiting solutions to detect and deter fraud are growing more sophisticated, affordable, and accessible.

This ebook examines many facets of brand protection – why it is necessary, how it works, who is vulnerable, how to implement an effective program, what to look for in a technology partner, and which emerging technologies will make a difference in the future.


Dark Arts: The Forms Counterfeiting Takes

Nothing erodes brand trust faster than disclosure of product falsification, recalls, consumer harm, or news of legal action against a brand. This can prove toxic to any popular brand. These outcomes often result from organized criminal activity in the supply chain. Criminals have a sophisticated network of willing players throughout the global supply chain in practically every industry. Profiteers typically target high-value products with strong consumer demand, and especially lucrative industries such as petroleum, pharmaceuticals, spirits, and health and beauty. Here's a quick look at some of the tactics used by criminals today:

- **Counterfeiting:** Products are produced to imitate the genuine offering using dangerous ingredients and presented as authentic.
- **Diversion:** Genuine products are smuggled or diverted without manufacturer authorization from lower-priced to higher-priced markets.

- **Tampering/Reuse:** Packaging or containers are refilled or reused with illegitimate ingredients or dosage with intent to deceive the consumer. This includes legitimate products that are expired, re-labeled, and misrepresented.
- **Adulteration:** For purposes of dilution or volume substitution, some dangerous or low-quality substances are added to genuine products, including fuel, oil, food, cosmetics, biologics, or other chemicals.

The less visibility and control a brand owner has over the supply chain, the more vulnerable products become to the risk of compromise. Therefore criminals target products distributed through complex and disaggregated supply chains. They can introduce counterfeit or diverted product at various points in the system without detection. Often impacted are premium products and popular brands where product demand is high or rapidly growing, and price points are at a premium. The result



can include inferior quality and faulty parts leading to consumer dissatisfaction, recalls, and huge safety problems.

Medical devices and supplies are another product category with far more lethal consequences. Growing numbers of fake medicines and testing equipment linked to coronavirus, for instance, are being discovered at an alarming rate, according to the WHO. In the same week COVID-19 was declared a pandemic, a fake and dangerous rendition of a popular potential therapeutic drug with a street value of more than \$14 million was seized by Interpol⁵.

Generally, perpetrators seek products with minimal authentication features. While many industries have advanced brand protection teams and policies, some industries have been slow to adopt a mature brand protection function, making them ripe for counterfeiting and tampering. Brand owners prepared to detect, measure, and prevent potential risk in their supply chain can minimize or avoid damage altogether.

Cutting a Wide Swath of Damages

It is forecast that by 2022, the negative impact of counterfeiting and piracy will drain US \$4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk. This impact cuts a wide swath across many industries and businesses including:



Pharmaceuticals and OTC Medicines: At least one million people die each year after consuming counterfeit medicines⁶.



Spirits and Premium Drinks: Counterfeit or illegal alcohol, recognized as “unrecorded” alcohol, is not monitored for quality or taxation. The WHO estimates that 25 percent of the alcohol consumed worldwide is unrecorded.



Tobacco: If the global illicit trade in tobacco was eliminated, governments would gain at least US \$31 billion in additional taxation revenue. Curbing this illicit trade could save over 160,000 lives annually by 2030 and beyond.



AgroChem: The WHO estimated that counterfeit and adulterated pesticides poison over three million people⁷ annually and result in over 200,000 deaths mainly in developing countries due to unregulated trade enforcement.



Health & Beauty: According to the FBI, counterfeit cosmetics have contained adulterants such as paint thinner, which irritates the eyes, nose, and throat in addition to being flammable and poisonous.



Automotive: Counterfeit parts cost the global auto industry an estimated US \$20 billion annually and put the lives of consumers at risk daily⁸.





Spotlight on Agrochemical

The Challenge

An agricultural brand owner of chemical active ingredients suspected one of its formulators was violating the licensing agreement by using a generic substandard ingredient for a licensed active component. The formulator also appeared to be diverting the end-product for sale in a region outside of its licensed territory where pricing was higher.

The Solution

Authentix developed a solution to detect use of the properly licensed active ingredient, at the correct concentration, to ensure enforcement of the license agreement. Authentix worked with the manufacturer to incorporate U.S. FDA-compliant in-product markers into the licensed active component, ensuring that the new marker could endure the harsh synthesis process, become homogenous and remain stable, while not impacting the active ingredient. A field test of the suspected formulator's end-product is conducted to quickly show either no active ingredient or a diluted concentration to prove the formulator was diluting or replacing the licensed active ingredient with a generic product.

The layered marker program allows widespread, quick field screening, with suspect samples sent to a centralized laboratory for validation to provide support for corrective action. The manufacturer's personnel were trained to use the test kits and perform the laboratory analysis, allowing them to monitor the formulator's end-product and enforce compliance with the licensing agreement.

The Outcome

The agricultural brand owner was able to determine conclusively that the formulator was in violation of its licensing agreement. The results of multiple field and lab tests enabled the agricultural brand owner to rapidly enforce the requirements on the formulator and ensure a compliant finished product, reduced complaints, and increased sales of the active ingredient.

Top Three Benefits of Brand Protection Programs

- **Protection of the brand owner's livelihood** – namely, its reputation and investments into market-leading proprietary products.
- **Consumer protection** – no brand owner wants their name associated with health hazards or calamities resulting from brand compromise.
- **Corporate citizenship** – companies that are proactive, deploy product protection programs, and are serious about a no-compromise climate, are more responsible corporate citizens.





Technological innovations have led to widespread outsourcing and high-quality manufacturing around the globe. Many brand owners have deployed this business model to see potential cost savings and scaling possibilities in delivery capability, lower facilities expense, and increase operating efficiencies. Now, innovation is hurting the same industries by enabling undetectable counterfeit goods to make their way into the supply chain. In China and India, illegal pesticides are believed to comprise up to 30 percent⁹ of the pesticide production. The rapid growth of chemical-manufacturing capabilities in many developing countries has made possible this unregulated manufacture and trade of branded pesticides - and it doesn't end there.

In Europe, nearly 17,000 tons and 8.7 million gallons of potentially dangerous fake food and drink¹⁰ were seized in a collaboration between Europol's Intellectual Property Crime Coordinated Coalition and Interpol. Tampered expiration dates on food products, controlled medicines added to drink products, and meat stored in unsanitary conditions were some of the offenses discovered during the operation.

You cannot ignore the rapid acceleration of online product sales and distribution via the internet. From licensed apparel and health and beauty products to medical devices and medicines, the reality is a huge opening to counterfeit products being

sold direct to consumers without authorization or approval. Counterfeiters are quick to exploit innovations in the e-commerce market to create "opportunity."

Case in point: Digital marketplaces – think Amazon, eBay, Etsy and countless other emerging online sites – are enabling and proliferating sales of counterfeit and knockoff goods.

Availability of counterfeit goods has shifted from gray markets such as sidewalk vendors and flea markets to mainstream e-commerce marketplaces. In fact, according to a 2018 study by the U.S. Government Accountability Office, about 40 percent of a sample of goods bought on popular e-commerce websites were fake. Data collected by the U.S. Customs and Border Patrol between 2000 and 2018 shows that seizures of counterfeit and pirated goods at U.S. borders, much of destined for e-commerce channels, has increased ten-fold¹¹.

In this climate many companies are thinking more broadly about how to implement coordinated anti-counterfeiting and anti-diversion strategies across their brands and throughout different regions of the world. Just as tamper-evident seals on bottles of pills and liquid formulations became more common after a tampering scare in the 1980s, attitudes toward anti-counterfeiting technologies are beginning to evolve.

Previously viewing such measures as an **"extra feature"** that only **"added cost"** to products, brand owners now realize the **importance of implementing** product risk assessment and adding security features to **protect the integrity of their brands** and, more importantly, ensuring their **customers' safety**.

Authentix[®]
The Authority in Authentication



Different Features, Unique Purposes

Anti-counterfeiting features that authenticate products are both overt and covert, and can be applied in numerous ways: in product and on product - on labels and closure seals, on cartons where containers of products are stored, into plastic parts of individual packaging, and even onto metal and glass components of packaging.

Each feature serves a unique purpose. Covert or invisible markings enable trained inspectors to quickly authenticate

genuine products in the supply chain, identify the source of diversion or determine other illicit activities. There are also overt features that allow the end consumer to verify the authenticity of their purchased product. When combined with careful design and production quality controls in authentic product manufacturing, these features raise the bar of complexity for counterfeiters and make the product a less attractive target and far less vulnerable.



Individual Security Features

Overt Security

Visible security features, also known as overt security, are valuable in product authentication. These features are visible to the naked eye or can be felt via touch. This category includes holograms, color-shifting inks and security threads that are difficult to reproduce or copy. Other examples include microtext, thermographic ink and even micro optics (the blue lenticular strip found on the current U.S. \$100 bill).

Although visible security features are a starting point, counterfeiters are creative. Even if a visible authentication feature is hard to recreate perfectly, a counterfeiter with the right tools and illegal intent only needs to copy it closely enough to confuse a consumer who just gives a package a quick glance. Additional features create layers of security - making it more difficult, even impossible in some cases, to copy or duplicate.

Overt Security Tactics

- Optically variable inks
- Pearlescent inks
- Gold and silver inks
- Anti-tampering technologies (tamper-evident closures and labels)
- Optical security technologies (holographic seals and labels)



Covert Security

High-security covert features can be embedded into labels, closure seals, or other features of product packaging. Although these covert markers are invisible to the naked eye, they can be found and measured with specialized handheld instruments using proprietary optics and detection algorithms for rapid, secure field authentication. Additional forensic layers of security can be embedded into materials and confirmed through more extensive laboratory analysis for evidence to further prosecute.

Semi-Covert Security

As the name suggests, these are features that might not be noticed until someone closely examines the product or package. They include:

- Pantographs
- Micro text
- Metameric inks
- Scrambled indicia
- Special-effect inks
- Coin-reactive inks
- Thermochromic inks

Forensic Security

Forensic analysis involves laboratory testing of products via an embedded (non-native) component or molecule added to a substrate or solution to determine authenticity. Unique product elements are examined so brand owners can generate compelling evidence of counterfeiting for legal proceedings. However, the ability to trace a product back to its origin is not supported unless a unique hidden tracing element is added to the product.

Covert Security Tactics

- Heat-activated inks
- Color-shifting inks
- Light-activated inks
- Fugitive inks
- Inks or materials with specialized fluorescing taggants
- Ultraviolet activated inks

Serialization

In the serialization process, a company applies individual unique codes and/or signatures at the point of manufacture (giving each product an identifiable attribute) and defines scanning locations where retrieval and association of the unit can be linked to the scanning transaction. These transactions uniquely capture, track, and store data from those markings to a managed database that allows authorized personnel to monitor the product journey by unit or larger groups. Most are familiar with this process as it applies to shipping a package overnight, when you can track it on the internet until it reaches its destination.



Digital Solutions

Digital authentication solutions involve the application of a unique differentiator to products – a code, number, or symbol that results in a digital ID. Each unique imprint is recorded in a database. In secure digital graphic authentication, a specialized code, symbol, or mark associated with a unique number or bar code is recorded. Variable product information highlighting product attributes such as manufacturing date and time, expiration dates, lot numbers, pictures, and a host of other origin information can be added to the database record and associated with the unique product. When the product is later scanned, a specialized smartphone application is needed to confirm that the unique identifying graphic is connected to that product and therefore is authenticated. At the same time, variable data is posted on the product's database record relating to the scanning event.

As the product travels through the supply chain, the unique number or symbol can be collected in the database and added to the database history. This information is available to a credentialed user via a mobile app or localized database. In a track and trace system, for instance, the information flow can be bi-directional, so the collection of the symbol, the scanning event and the unique call to the database can be recorded and appended to the product record for verification purposes.

There is a range of complexities associated with these digital systems. Some can be a simple yes/no result on authentication. Others can show the complete variable information, including a detailed accounting of product movement in the supply chain all the way to retail purchase and ultimate deactivation of the product's unique ID number.

RFID

Another digital tool available is Radio Frequency Identification (RFID), which is usually a small antenna and receiver system where a unique product-level ID is hidden or embedded in a small chip or printed label. In some cases, the chip residing on the product can have its own power source (active) or can be energized through the collection device (passive). The ability of these "electronic labels" to communicate with a centralized database system performs like other track and trace systems.

However, RFID can be expensive on a per-product basis and has limitations on many applications, including potential interference with the signal via ambient conditions. It should be noted that track and trace systems are not able to detect materials that move covertly or surreptitiously around legitimate supply chains, such as when counterfeit products are distributed through e-commerce.

One and Done? Not So Fast.

Today's reality is that one level of security is rarely sufficient. Counterfeiters' technology is constantly evolving, so a simple one-dimensional technology to combat their efforts isn't enough - it takes an arsenal of tools.

An effective multilayered approach in which overt, covert, and forensic features are applied is the most effective long-term solution to detect and deter counterfeiting. These features can be incorporated into labels, closure seals, storage cartons, plastic, metal, and glass packaging at very reasonable costs. Each type of feature serves a unique purpose, from color-shifting inks that allow end-users to quickly identify a branded product as genuine to covert markings that enable an inspector to identify many factors involved with the source of authenticity.

Multilayered Options

- Authentication
 - Overt
 - Covert
 - Forensic
- Online monitoring
- Analysis – data collection and insight
- Intellectual property and trademark enforcement



Spotlight on Pharma

The Challenge

Counterfeit copies of a major pharmaceutical brand turned up in the U.S. market. No security measures were in place to allow patients or inspectors to discern what was authentic and what was counterfeit. Consequently, \$1 billion worth of the product, already in the distribution pipeline, could not be sold—at least not until the brand owner implemented a way of allowing patients and retailers to verify the authentic medicine. Patient safety, the company's hard-won reputation, and roughly \$1 billion in inventory were at risk.

The Solution

Teaming with Authentix, the company repackaged its product to include a variety of authentication features that could be identified by patients and inspectors, both in the field and in the laboratory. These included:

- Overt, color-shifting inks readily recognized by patients, and pharmacies.
- Covert, machine-readable inks detectable in the field by inspection staff with appropriate readers.
- Forensic markers detected under laboratory analysis.

The Outcome

The solution provided a secure means of instantly identifying an authentic product from counterfeit versions. The benefits were immediate and significant:

- \$1 billion worth of “frozen” product was released for sale.
- The expense of a full product recall was averted, saving millions of dollars.
- The customer was able to mitigate the risk of potential lawsuits and reputation issues.

Most importantly, confidence in the brand was restored among physicians, pharmacists, and patients.





A Winding Path: Identifying and Implementing an Effective Brand Protection Program

With illicit activities on the rise, the stakes are getting higher across all industries. Understanding the risks associated with high-value products such as medicines is vital to protecting public safety and brand integrity. It is increasingly important to ensure the viability of secure products in your supply chain and to close the gap on counterfeit products. Proactively identifying what products are at risk of being counterfeited is the first step in understanding potential threats.

The truth is that no one solution or security measure will be able to fully prevent counterfeiting across the global marketplace. However, each brand owner can define the risks and corresponding appropriate controls to minimize and deter compromise. The key is comprehensive risk assessment and the selection of a solid partner offering a full suite of technology and service solutions that can scale to your business needs.

Five Steps to Defining Risk of Product Compromise

Risk management can be time-consuming and labor-intensive when you are looking to preserve your brand and the customers who depend on you.

1) Identify risk areas

First, when identifying product risk, develop a risk inventory for your products. The level of risk associated with each product will differ depending upon a multitude of factors, including supply chain complexity, geography in which the product is sold, price points, margins, complexity to copy, and total demand expected for the product. To identify vulnerabilities and risk, consider the following questions:

- Is my product high in volume and low in variable cost? If so, then it can be a prime target for copy and resale.
- Is my product sold at high gross margins? If yes, then regardless of its price, it will be an attractive target to counterfeiters looking to benefit from the marketing efforts of legitimate manufacturers.
- Does my product have a large market share? If yes, then it stands to profit a great deal from positive changes in the market – making it more appealing to imitate.
- Does my product and/or packaging have security features? If no, then there is little to deter counterfeiters from targeting your product.

- Is my product distributed through a complex supply chain? If yes, then there are multiple opportunities for counterfeit products to enter.
- Is my product sold online or manufactured in countries known for fraud? If yes, then you have the potential for compromised manufacturing at the local level and the possibility to lose control over distribution.

Your priorities are to identify your highest value products and assess the reliability of your supply chain to understand your brand's exposure to fraud or compromise. While you should

always attempt to identify every real risk, not all vulnerabilities will be countered with the same level of resources. Instead, resources should be focused on risks that warrant the expenditure. This can be calculated by comparing the severity of a risk's impact with the likelihood of its occurrence. A potentially disastrous risk – harm to a consumer, for instance – with a high probability of occurring should rank at the top of your assessment, while a mild and unlikely risk shouldn't necessarily be prioritized.

2) Assess risk

The second step is to assess the likelihood, impact, and overall threat of each risk factor.

You should first determine how susceptible

each product in your portfolio is to an attack. Use this information to create a high-risk portfolio by applying a three-part system of assessment to achieve the following:

- Aggregates risks
- Assesses potential brand damage
- Maps the supply chain environment

First, aggregate risks and the factors that comprise each individual risk. Score each product on its risk areas and weight each indicator. The indicators can be adjusted and altered, but this process of categorization will provide you with a prioritized list.

Next, assess potential brand damage. With brands among the most valuable assets a company owns, the fragile bond of trust between consumers and their products is a corporate and strategic asset that cannot be risked. Any injuries or deaths caused by counterfeits can destroy this relationship, and top management should be aware of the risk and committed to demonstrating leadership on the issue. Brand protection managers and marketing also should be involved and participate in assessing the risk of counterfeit attacks and the value of all proposed strategic solutions.





Lastly, any exposure in your supply chain should be mapped, understood, and corrected.

3) Develop a risk management strategy

Once you've completed your risk assessment and vulnerability analyses, you should examine the resulting information and create an integrated risk management strategy for each high-risk product that addresses the following:

- Define a set of policies and procedures to ensure that the organization's risk profile becomes properly followed.
- Segment product risks by specific threat; for example, consumer safety vs. losses from diversion activity.
- Identify the points in the supply chain where threats are the greatest.
- Define the areas of highest vulnerability, identifying best practices for action – for example, policy changes for packaging requirements.
- Recognize risk scenarios and how to detect those when they occur.
- Allocate resources appropriately based on risk areas.
- Draft a communications plan that covers potential causes of risk, avoidance actions, transference and mitigation actions, and potential impacts and contingency actions.

4) Create an action plan

At this point, responses to the most pressing threats can be translated into action by organizing a method for management, information, and technology tools to respond to threats. This broadly falls into the following three categories:

- Detection and deterrence
- Enforcement
- Prosecution

Detection and deterrence involve the application of programs that communicate how your company is protecting its products and its commitment to prosecuting offenders. This can deter a large fraction of these threats, with possible approaches including:

- Security features on the packaging – overt, covert, forensic, tamper-evident, serialization and/or track and trace.
- Well-executed public relations education and awareness campaigns.
- Supporting efforts that increase the statutory penalties associated with this crime.
- Incorporating contractual language in vendor agreements that penalize actions detrimental to both your policies and your efforts to combat counterfeiting.

- Unannounced audits of downstream distribution partners.

Enforcement is the pre-determined action you plan to take upon the discovery of a specific type of adverse event. The strategy depends on various elements such as the geographic location of the event, resources available in those areas, and local laws and regulations. Detection of an adverse event should align with action and follow-through. Corporate policies should be clear and enable those responsible for mitigating the attacks to use technologies that will fight attacks in a cost-effective and operationally efficient manner.

Prosecution is the end game after a serious attack. Steps taken are intended to support investigative and forensic efforts to protect your brand. Having legally defensible evidence presented in an organized fashion with evidentiary value in the courts is vital in civil and criminal litigation – and, in absolving your company of culpability. Approaches may include:

- Multiple integrated authentication technology components implemented in areas that represent the highest threat potential.
- Integrated web, field, and analytical systems to alert the company early in any attack, allowing for early intervention.
- Flexible investigative field force that can be quickly scaled and focused at the right place and time.
- Method for timely and accurate communication, both internally and externally.
- Accountability tool that facilitates analysis and reporting concerning the impact of both the technology and operational methods.

5) Monitor risk and continually re-evaluate your strategy

The last step in your strategy involves collecting and monitoring information. Data analytics offer an opportunity to better understand risks, see vulnerabilities, and respond promptly and proactively. Today, data visualization technology is critical in the fight against illicit brand activity. Relevant data can be collected, analyzed, and acted upon based on insights revealed in dashboards – from counterfeit hotspots to analysis of unit-level product data.



The current counterfeit landscape is a “not if, but when” environment. As a result, your strategy should be robust, well-researched and well-implemented to quickly authenticate and act on issues uncovered or predicted. One of the most effective deterrents to risk is teaming with a partner with the requisite skills, experience and talent to assist you in all facets of brand protection.



How to Select a Brand Protection Partner

Brand protection partners will work with you to develop, implement, and manage a proactive strategy to detect, identify, and deter counterfeiters. But what should you look for in a partner? The following are key considerations when you are vetting an authentication expert.

Your Business is Their Business

Choose an authentication partner that understands your business and offers consultative services—it's critical that your partner has experience with your products and understands your industry. Your partner should fully understand the challenges you face, articulate your exact problems and work with you to set goals for your program. A trusted relationship should be able to demonstrate:

- Common vision for the goals, resources, and time management of your authentication plan.
- Knowledge transfer on key topics such as global regulations and advanced technologies.
- Development of a realistic risk assessment matrix.
- Proactive approach to managing your supply chain and preventing problems.

Thorough Risk Assessment Plan

Determining the appropriate level of security required for a given product requires a thorough risk assessment strategy. The strategy provides insight into the risks you face, the nature of product distribution, your partners in the supply chain, and the goals for the branded product. Certain fast-moving consumer goods and pharmaceuticals, for instance, may warrant a high-

level security solution (such as a security taggant ink and reader system). Conversely, common consumer items might warrant a lower-cost, lower-level security solution.

The appropriate security level depends on the annual amount lost to counterfeiting and the value of the product to the brand owner. Determining the appropriate level of security to mitigate a counterfeiting issue must be based on a thorough assessment and discussions with your authentication partner.

Customized Solutions

Select an authentication partner that can fully customize a solution to fit not only the unique challenges of your industry, but also the needs of your specific organization. For instance, your partner should have the necessary expertise on the types of security features needed for different types of product packaging, such as tamper-evident seals, foils, labels, etc. Be sure to look for a partner offering:

- State-of-the-art color marking systems
- Multilayered security features
- Monitoring and enforcement plan
- Ability to function properly in a multi-channel distribution environment
- Data capabilities – dashboards, cloud platforms



Multilayered Approach

Decades of experience have proven that there is not a simple “silver bullet” technology that can be applied to all products for perfect brand protection security. As discussed earlier, a multilayered approach in which overt, covert and forensic features are applied in various ways is the most effective long-term solution against counterfeiting.

Supply Chain Integration

More than likely, your current supply chain is complicated and has many moving parts. An effective authentication partner should be able to instantly integrate within that chain. In addition, the partner should be a “third-party agnostic” solution integrator without any prejudice towards other links in your supply chain. This partner will be able to objectively analyze your supply chain, identify potential problems, and recommend ways to correct issues they’ve uncovered.

Print Trials and Authentication Support

An experienced authentication partner should be able to certify and conduct print trials with your manufacturing printers. All manufacturing of security materials should be produced in a secure facility under full chain-of-custody protocol. A security audit is the best way to determine this. The brand owner must be confident that appropriate physical security and auditing procedures are maintained in the potential partner’s facility. It is important to only work with a partner with quality accreditations appropriate for the subject matter and technologies involved.

Talent and Reach


Your authentication partner should have technical and commercial teams to provide the appropriate level of expertise required to authoritatively advise on the features of their technology and its implementation. In the case of a global brand, your authentication provider should have a global footprint. This includes global reach for delivery, servicing, technical support, dealing with customs and regulatory expertise to deal with regional and country-based compliance issues.

Implementation Strategy

Some potential partners might be great at strategy and planning and inferior at implementing those plans. It’s important that the partner provides extensive documentation of their experience with implementing a strategy, including a resume consisting of several multi-year customer relationships. In addition, your partner must agree to become an integrated part of your team and extend that support to your third-party vendors.

Committed Partner

An authentication partner must be willing to see you through the good times and challenging ones, too. You need an ongoing relationship with your partner to stay one step ahead of counterfeit issues. An established, trusted strategy is the only way your program can sustain long-term success.





Spotlight on Fast-Moving Consumer Goods

The Challenge

A global hair care manufacturer produces category-leading brands with high consumer loyalty and demand. Their products are marketed through exclusive, professional beauty care channels via a complex supply chain with diverse manufacturing systems and multiple distribution outlets.

All these elements make their products high-value targets for counterfeiters, organized theft rings, and gray market wholesalers. In fact, the manufacturer found they were being negatively impacted by diversion of its products from legitimate distribution channels into gray or retail markets. This situation was creating dissatisfied customers and weakening their market promotional efforts.

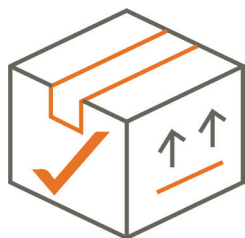
The manufacturer needed an anti-diversion authentication solution that would help them maintain brand equity. It was imperative that the solution include the ability to authenticate the product and verify “product genealogy” throughout its life cycle. They also needed the ability to track product throughout their entire supply chain and make sure the right product was always delivered to the right location.

The Solution

The global hair care manufacturer turned to Authentix to implement an authentication solution of serialization and a track-and-trace system that identified product diversion in the brand’s distribution channels. The solution utilized multiple covert authentication features that allow item-level serialization, full product traceability from manufacturing to retail, and provisions to track repackaged products. In addition, the track-and-trace system was seamlessly integrated into manufacturing process controls for all of the manufacturer’s 13 production lines. Itemized serialization was accomplished for over 165 million products, enabling full traceability from manufacturing to retail.

The Outcome

- Successfully identified channel leaks within a complex distribution chain of over 2,500 channel partners and 15 distributors.
- Over 300 million units were marked since the Authentix solution was implemented.
- 47 percent reduction in product diversion and a consequent increase of \$77 million in sales.





The Future of Brand Protection

More and more, the ubiquity of technology enables counterfeiters to produce higher quality products that mask inauthenticity. Brand owners must begin to think differently about their supply chains and how to secure them. This not only means working with trusted partners across the supply chain, but also deploying advanced tools and technologies for brand protection. Yes, it means fighting fire with fire. This is the future of brand protection.

Artificial Intelligence and Machine Learning

While still in the early days of adoption, artificial intelligence (AI) is being applied in some areas of brand protection. Using machine learning, for instance, computers can analyze and learn from large, complex datasets, recognizing patterns that reveal potential fraud. Packaging can be analyzed, along with data compiled from sensors. Anomalies the human eye cannot see can be detected and offenders can be flagged.



Artificial Intelligence in Authentication

Examples of strong and weak applications of artificial intelligence to authentication.

Strong

- Quickly identify item types
- Optimize algorithms used in hologram authentication
- Detect design variation
- Detect variation in manufacturing
- Create “codes” from random patterns

Weak

- Any problem where good data sets are unavailable
- Items with high manufacturing variation
- Items with high design variability or changes
- Items with physical degradation



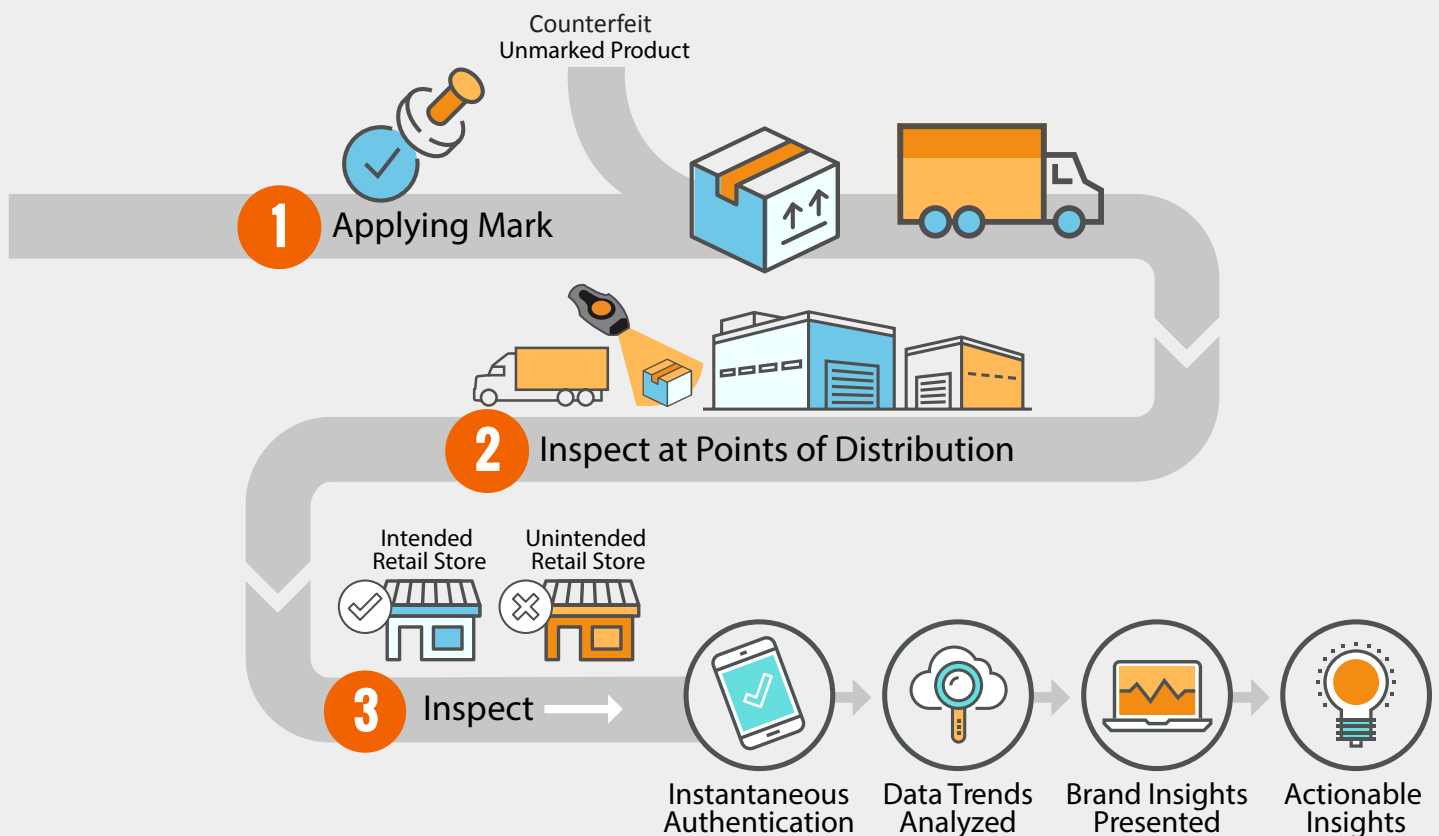
Data and Digital Platforms

Data is the oil in the engine of many enterprises today. But few are applying this lubricant to brand security, with the notable exception of Authentix.

Yes, companies are investing in supply chain and inventory management data to optimize production. But for the most part, brand security is a missed opportunity. As data collection technology improves and is more available to consumers – think smartphone cameras for image collection, for instance – more brands can turn consumers into data collection agents. High-resolution photos, for instance, can be taken of in-store products and sent to brands for analysis.

The value added through a reliable flow of accurate and timely data provides actionable insights stakeholders can use to measure and reconcile information quickly, as well as react to and remediate illicit activities, securing the supply chain.

An Effective Supply Chain





Right Data, Right Time

Having the right data at the right time will speed reaction times, enable faster diagnosis of issues, and deliver a more complete understanding of corrective actions to take. For instance, the Authentix AXIS® Brand Protection technology is a cohesive data platform that collects, stores, and analyzes data to help companies make informed decisions on brand protection issues. This is a secure, comprehensive, cloud-based, end-to-end platform designed to deliver a complete picture of your authentication efforts and results. It also provides actionable insights and helps identify counterfeit hotspots as evidence for responsive enforcement action.

Conclusion

If the past is prologue to the future, a tsunami of counterfeit goods is making its way into the global marketplace right now – from luxury items and medicines, to food, spirits, auto parts, and more. The damage they can cause is incalculable, including loss of human life, degraded consumer safety, and obliteration of brand trust.

So whether you choose to invest in emerging technologies and teams of on-staff talent to protect your brand – an endeavor that could cost millions of dollars annually – or team with an experienced third-party provider such as Authentix, taking decisive action is essential to the health of your brand, your revenue stream, and your consumers. Risk will continue to grow as the arsenal of tools that criminals employ expands.

The only way to stem the tide and mitigate risk is an intense focus on brand protection. No company can survive without it.



Sources

1. <https://iccwbo.org/media-wall/news-speeches/global-impacts-counterfeiting-piracy-reach-us4-2-trillion-2022/>
2. https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf
3. <https://monroescoop.com/uncategorized/84493/authentication-and-brand-protection-market-2020-size-key-players-demand-supply-growth-and-forecast-to-2026/>
4. <https://iccwbo.org/media-wall/news-speeches/global-impacts-counterfeiting-piracy-reach-us4-2-trillion-2022/>
5. <https://www.bbc.com/news/health-52201077>
6. <http://scienceinpoland.pap.pl/en/news/news%2C28780%2Cexpert-counterfeit-drugs-kill-1-million-people-each-year.html>
7. https://www.washingtonpost.com/world/the_americas/in-agricultural-giant-brazil-a-new-and-growing-hazard-the-illegal-trade-in-pesticides/2020/02/09/2c0b2f2e-30b3-11ea-a053-dc6d944ba776_story.html
8. <https://medium.com/@veridocglobal/eliminating-counterfeit-auto-parts-89c50533cba5>
9. <https://edis.ifas.ufl.edu/pdffiles/PI/PI21000.pdf>
10. <https://www.europol.europa.eu/newsroom/news/over-%E2%82%AC100-million-worth-of-fake-food-and-drinks-seized-in-latest-europol-interpol-operation>
11. https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf

About Authentix

As the authority in authentication solutions, Authentix thrives in supply chain complexity. We provide advanced authentication solutions for governments, central banks and commercial companies, ensuring local economies grow, banknote security remains intact, and commercial products have robust market opportunities. Our partnership approach and proven sector expertise inspires proactive innovation, helping customers mitigate risks to promote revenue growth and gain competitive advantage.



CORPORATE HEADQUARTERS

4355 Excel Parkway, Suite 100
Addison, TX 75001

www.authentix.com

NORTH AMERICA | EUROPE | MIDDLE EAST | AFRICA