Authentix®
The Authority in Authentication

WHITE PAPER

PRODUCT AUTHENTICATION:
A 5-STEP RISK ASSESSMENT

Understanding the Landscape

Counterfeiting and piracy are highly pervasive across countries and sectors, representing a multi-billion-dollar global industry that continues to grow. With these illicit activities, the stakes are high. The consumers' health and safety are on the line as millions of dollars' worth of products are transported from one country to another.

Due to a complex supply chain, understanding the risks associated with these high-value products is vital to protecting public safety and brand integrity. It is therefore increasingly important to ensure the integrity of your supply chain, and to close the gap on counterfeit products. Proactively identifying which products are at risk of being counterfeited is the first step in understanding potential threats.

You may not be able to fully prevent counterfeiting across the global marketplace. The goal is to define appropriate controls to minimize the risk of counterfeit products. This white paper will provide you with five steps to sharpen your risk assessment strategy.

Negative impacts of counterfeiting and piracy are projected to drain US$4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk by 2022.

(Source: International Chamber of Commerce)

Structuring Your New Strategy

The starting point must be evaluation of the risk, its potential consequences, identifying a core team for confronting the problem, and multiple party input so the strategy reflects different considerations from across the organization. This is the required groundwork for a proactive approach in understanding the risks within your organization before they happen.

70% of counterfeit products are purchased from online marketplaces.

(Source: Better Business Bureau, May 2019)

1. Identify Your Risk Areas

The first thing you should do when identifying your risk areas is to develop a risk inventory that can be designed around your portfolio of products. The level of risk associated with each product will differ depending upon a multitude of factors – including the complexity of its supply chain, its monetary value and the demand for it. There will be numerous other factors for each unique product and business, but the risk inventory can be broadly mapped using the following questions:

- Is my product high in volume and low in cost? If so, then it can be easily copied and sold in large numbers.
- Is my product in high demand? If it is, 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 it does, then it stands to profit a great deal from positive changes in the market – making it more appealing to imitate.
- Does my product lack security features? If so, then there is little to deter counterfeiters.
- Does my product experience a complex supply chain? If it does, then there are multiple opportunities for counterfeit products to enter.
- Is my product sold on the internet? If it is, then you have the potential to lose control over distribution.

Your priorities should always be to identify your high-value products, assess the reliability of your supply chain, to understand your brand's exposure and to anticipate lost revenue.

While one should always attempt to identify every real risk during this period of assessment, not all risks will be countered with the same level of resources. Instead, resources should be focused on those risks that warrant the expenditure. This can be calculated by comparing the severity of a risk's impact to the likelihood of its occurrence. A potentially disastrous risk with a high likelihood of occurrence will rank extremely high in your assessment, whilst a mild and unlikely risk will be far from a priority.

Disadvantages of a Reactive Approach

1. Authentication is not in place.
2. Company resources are unpredictably impacted.
3. Lack of control over costs heavily impacts the budget.
4. Processes are unknown.
5. The supply chain is weak.
6. Distribution chains remain unclear.
7. Departments are fragmented.
8. No checks and balances are in place.

It may also be beneficial to separate the notion of risk into several different categories, with each tied to specific types of threat. The goal is to develop a set of responses that can minimize the damage and enhance the company's ROI, consumer safety and brand integrity. Risk assessment is also about being proactive, understanding the risks associated with your high-value products, and knowing how to respond.

Risk Category	Threat Examples	ROI Benefit
Revenue loss	Counterfeiters stealing sales, R&D investment, and marketing expenditures by selling counterfeited, adulterated, and diverted products.	Revenue recovery
Unnecessary costs	Undue drain on management resources, uncertain response during a product attack, and slow investigative cycle or unnecessary recalls.	Cost reduction and avoidance
Liability	Potential penalties, litigation costs, and damage awards.	Liability avoidance
Brand erosion	Loss of consumer trust, erosion of brand loyalty and brand premium price, and loss of market share.	Brand protection and enhancement

The importance of a proactive approach can be seen in the Procrit counterfeiting incident, highlighted in Authentix' on-demand webinar. Counterfeited in 2002, the Procrit manufacturer's reaction was rapid, but the counterfeit products still caused massive disruption to the company and their supply chain—because they were in a reactive, not proactive mode.

2. Assess the Risk

The second part of your assessment process should be to assess the likelihood, impact, and overall threat of each identified risk factor associated with your high-value products. You should first determine how susceptible each product in your portfolio is to an attack and use this information to create a high-risk portfolio. But where to focus? And how to prioritize your risks? These are the questions many of those attempting to implement a risk strategy may be asking themselves – questions that can be answered by following a simple, three-part system of assessment:

- Aggregating risks
- Assessing potential brand damage
- Mapping the supply chain environment

The first thing you should do is aggregate risks and the factors which make up each individual risk. Each product should be scored on its risk areas, as discussed earlier in this report, with each indicator then being weighted. The indicators can be adjusted and altered, but this process of categorization should provide you with a prioritized list.

You should then assess the potential brand damage. With brands amongst the most valuable assets a company owns, the fragile bond of trust between consumers and their products is a corporate and strategic risk. 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 should also be involved and should form part of a team involved in assessing the risk of counterfeit attacks and the value of all proposed strategic solutions.

Typical questions you may wish to consider when working as part of the team assessing potential brand damage could include:

- What would be the impact if company investigators could not determine the authenticity of a suspicious product in the field and how beneficial would it be for them to be able to do so quickly and reliably?
- If a major counterfeiting incident occurred within your company, how beneficial would it be for your top management to be able to describe a security check that consumers and law enforcement agencies could do to verify the authenticity and safety of their products?

3. Develop a Risk Management Strategy

Once you have completed your risk assessment and vulnerability analyses, you should examine the information and create an integrated risk management strategy for each product of sufficiently high risk. The intent is to analyse the organization's situation so that specific action plans can be developed and pursued. The following strategy will provide you with a better-informed risk decision-making process:

- Define a set of policies and procedures to ensure organizations risk profile is followed
- Segment product targets by specific threat, for example – consumer safety
- Identify the points in the supply chain where threats are the greatest
- Define your areas of greatest vulnerability, identifying best areas for action – for example, policy
- Recognize risk scenarios
- Allocate resources appropriately
- Draft a communication plan which covers potential causes of risk, avoidance actions, transference and mitigation actions, and potential impacts and contingency actions.

4. Develop a Plan of Action

We are now at the point of the strategy where the 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, which we will look at in detail:

- Deterrence
- Enforcement
- Prosecution

Deterrence involves the application of programs that communicate how your company is protecting its products and committed 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-evidences, serialization and/or track and trace
- Well-executed public relations education and awareness campaign
- 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

> "Counterfeit makeup often contains known carcinogens arsenic, beryllium, and cadmium,"
>
> – Dr. Bobby Buka, a dermatologist in New York City

Enforcement deals with the large majority of threats that may be coming from more committed criminals. These criminals will not be deterred and will continue to pursue the potential profit. Combating these threats require a more aggressive, enforcement-oriented strategy supported by appropriate technologies. 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. Approaches may include:

- Multiple integrated authentication technology components implemented in areas that represent the highest threat potential
- Linkage that connects those responsible for managing risk, to field and other alert information, allowing the investigation of resources facilitating operational flexibility and speed
- 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

Unlike the previous two categories, prosecution is of value after the attack and is intended to support investigative and forensic efforts. Having legally-defensible evidence presented in an organized fashion that is recognized as having evidentiary value by the courts becomes vital in civil and criminal litigation.

Risk has three components

Risk is defined as the combination of the probability of occurrence of harm and the severity of that harm:

1. What could go wrong?
2. What is the likelihood of something going wrong?
3. What are the consequences?

5. Monitor Risks and Re-evaluate Your Strategy

The final part of your strategy should involve the collection and monitoring of information. A major aspect of this is data analytics, which presents an opportunity to better understand risks and to respond promptly.

You should first endeavour to conduct a risk review, during which the output and results of the risk management process should be reviewed, considering any new knowledge or experience. Once a quality risk management process has been initiated, it should continue to be utilized for events that might impact the original quality risk management decision. This should apply to events that are planned – such as the results of product review, inspections, audits, or change control – or unplanned – from root cause from failed investigations to recall.

The frequency of any review should be based upon the level of risk. Risk review might include reconsideration of risk acceptance decisions.

Final Thoughts

The current counterfeit landscape is a 'not if, but when' environment. The complexity of your supply and distribution channels provides a greater opportunity for the counterfeiters to thrive. Your strategy should be robust, well-researched and well-implemented in order to quickly authenticate suspicious products in the field. Consumer safety is paramount, and you need an authentication partner that can guide you in meeting your risk assessment needs.

"Companies that effectively leverage data analytics for forecasting and monitoring throughout the product life cycle are able to identify risks in real time and position the organization for a prompt response."

- Authentix Brand Protection Group

Authentix®
The Authority in Authentication

Work with Authentix

Let Authentix help you manage risk rather than react to problems. We thrive in supply and distribution chain complexity, providing innovative authentication solutions that help you effectively mitigate risks to promote revenue growth and competitive advantage.

Authentix®

The Authority in Authentication

CORPORATE HEADQUARTERS
4355 Excel Parkway, Suite 100
Addison, TX 75001

www.authentix.com

NORTH AMERICA | EUROPE | MIDDLE EAST | AFRICA