Authentix®

Anti-Counterfeiting
Brand Protection
Fuel Marking

Why Inspector-Led Authentication is Here to Stay

(and Better Than Ever)

Counterfeiting is a real and growing problem that continues to pose a risk to public safety and the reputation of brand owners.

Let's have a conversation.

Table of Contents

Brand Protection, Already a Complex Dialogue

Choosing to protect your brand from counterfeiters should be an easy decision for brand owners, one would think. However, it is a decision that touches every function within a product company: supply chain, operations, marketing, sales, and legal. And not everyone is convinced that counterfeits are a problem in their business or that the problem is big enough to invest in a solution.

This “is the problem worth solving” dialogue is most common to products that do not impact life safety or brands that do not compete and win in the marketplace on brand equity. During this problem-sizing phase of a customer engagement is when return on investment (ROI) calculations are made and brand owners begin to understand the impact of counterfeit products on revenue.

Once a company is convinced that counterfeiting is a problem worth solving, then the dialogue shifts to how to best solve this problem – and there are as many differing opinions as there are solutions. Brand owners are faced with considerations from ease of implementation, cost, robustness and reliability, and an overt versus covert strategy, just to name a few.

Thus, it is not a surprise that assisting a product company with a brand protection strategy can take well over a year from the time of first engagement to when the security features are in circulation.

The Evolving Role of the Consumer in Authentication

The ubiquity of mobile devices and improvements in camera quality and device capabilities has renewed conversations about the role of consumers in product authentication. We believe that engaging the consumer in product authentication is a positive step, but it is a step that requires a great deal of forethought.

Consumer authentication can serve as another layer in a well-designed multi-layer brand protection program, but brand owners should not delegate responsibility for securing their supply chain to consumers.

To begin, consumers do not want to scan QR codes. Marketing data reveals only 11% of consumers have used a QR code even when enticed with coupons, discounts, and loyalty programs. Moreover, QR code-based loyalty programs lose 60% of their customers in the first three months and 25% of apps are used only once and then never used again[1]. With these results, brand owners cannot expect to collect sufficient data to enforce a quality brand protection program if relying only on consumer data.

Second, consumer authentication leads brand owners into unknown waters. A common marketing concern while implementing security features on a package has been the loss of real estate to the security feature. Marketing has now lost valuable packaging space on which to brand and promote the product. With consumer authentication, marketing and legal will need to confront the potential brand impact of a false positive or, more dangerous, a false negative.

Today a false positive read by an inspector or quality auditor can be verified with further analysis or additional sampling. In the hands of a consumer one false positive could translate into a lost customer and a likely social media backlash risking thousands of current and future customers.

Conversely, what is a company's liability in the case of a false negative. Said another way, what happens when a brand sponsored authentication tool incorrectly authenticates a fake? What happens if that fake has real life safety implications?

These are only two examples that illuminate why brand owners are not ready for consumer authentication.

[1] Thanx, Branded App Case Study, April 5, 2016, http://blog.thanx.com/thanx-branded-app;
Simpson Carpenter QR Code market study, referenced in "Consumers "apathetic" about QR codes, https://www.marketingweek.com/2011/09/02/consumers-apathetic-about-qr-codes/

Consumer authentication can be wrapped into a more comprehensive marketing and brand engagement tool. However, it should be considered the last line of defense in a brand protection program and it should not divert resources and focus from brand owners securing their supply chains and ensuring counterfeits do not infiltrate legitimate retail outlets.

Internet of Things (IoT), Data Aggregation and Actionable Insights

If consumer level authentication is not yet the answer, then what can brand owners do to fight counterfeits? The answer is all around us and in the news everyday – upgrade your security feature to act as a real-time sensor in an IoT framework. When we collect real-time results we are able to see patterns, and when we see patterns we are able to take action.

The answer is not to equip consumers to authenticate products in legitimate sales channels. The answer is to prevent those counterfeits from making it to the shelves of legitimate retailers. To accomplish this, brand owners need to focus on how to get more sampling and testing completed of the products before they get to the shelves. Or, understanding through data what locations should be tested more frequently.

Real-time actionable insights can alert and identify hot spots of counterfeiting activity enabling brand protection investigators to focus resources and quickly contain the impact of counterfeit products. If a consumer finds a counterfeit product you can bet they will be tweeting, Facebooking, and Instagramming your brand and blaming the retailer before a trained inspector can validate results. This negative attention will only force your investigation to play out publicly in the media.

Improvements in Inspector-Led Tools

Inspectors need the right tools in the field to quickly identify counterfeit product and, in some instances, be able to validate the product is fake to authorize immediate action. For this reason and more, inspectors have long valued the presence of covert chemical markers (“taggants”) for their security robustness and reliability.

The most robust covert security features utilize a “lock-and-key” approach to marker and reader development, the markers are custom-made to work with a specific reader. This combination enables the security technology company to incorporate a third level of security, a chemometric model. The chemometric method the company uses both obscures the marker signature and the method used to read that signature. If a security feature uses off-the-shelf readers, the security feature may be more vulnerable to hacks and spoofs.

Like all technology, electronics and electronic components continue to get smaller, faster, and less expensive. Readers for authentication are no different. These devices can now fit discreetly in a pant pocket and weigh less than a few ounces. Cost is no longer an obstacle in deploying reliable readers to hundreds of inspectors.

Authentix has been a market leader in the development of covert security markers for twenty-years and provides covert machine readable features to many of the world’s leading central banks. We apply that elite experience to advancing our brand protection offering.

Used in conjunction with inspector scheduling features, the real-time data now available enables inspectors to be more productive, electronically creating case files and reports in hours. Data that once took days or weeks to compile and analyze, now takes seconds.

The Return-On-Investment Paradox

There exists a ROI tipping point for brand owners investing in covert security features. Invest too little in sampling and testing and not enough counterfeits are found to obtain actionable insights or deliver the desired ROI. Increase the testing and sampling and the rate of counterfeits identified increases, allowing the source of those counterfeits to be rooted out.

We have seen companies take the approach of invest a little, measure results, and then evaluate future level of investment based on program ROI.   This approach almost always delivers disappointing results. Brand protection is not a dip-your-toe in the water experiment. To be successful brand owners must commit to protecting more product with inspector-level authentication features.

Equally as important, and too often underinvested, is the corresponding sampling and testing of products to proactively audit the supply chain and retailers. The best security feature will not deliver a ROI if no one is validating its presence. Thus the return on investment paradox: invest too little and the program will not return its value.

Conclusion

Let us not confuse this already complex conversation with pushing the responsibility to the consumer to fight counterfeits.   Counterfeiting is a real and growing problem that continues to pose a risk to public safety and the reputation of brand owners.   The conversation should be about how we enable more sampling to be conducted by trained inspectors *before* the counterfeits make it to the shelves and before placing consumers at risk.   If consumers are warily scanning a product and questioning a product's authenticity on the shelf of a legitimate retailer, then brand owners have already lost.

Published by

Authentix

+1.469.737.4400

info@authentix.com

4355 Excel Parkway, Suite 100

Addison, TX 75001 USA

About Authentix:

Authentix is a leading global authentication and information services company. Authentix develops and markets Authentix Sherlox™, an end-to-end authentication offering for brand owners that includes an integrated system of security markers and readers, a powerful data information system, and robust services.

Learn more about what Sherlox can do for your brand protection program at http://authentix.com/offerings/sherlox/