THE PROMISE OF CONNECTED PACKAGING—FROM BRAND PROTECTION TO CONSUMER ENGAGEMENT

An unfolding revolution in digital packaging creates a trifecta of opportunity for brand owners

Avi Chaudhuri, PhD
Chief Scientist, Systech

Introduction

It is now well accepted that virtually all brands, from the utmost recognized to the newly eager, face an unprecedented onslaught of counterfeiting and gray market trading. In emerging countries, this menace is bold and audacious, with outright fakes appearing in the open marketplace. In developed countries, the problem is equally insidious due to online propagation of counterfeit products through e-commerce platforms.

In addition to counterfeiting there are two other challenges that concern brand owners. One of them is how to keep pace with the recent trend in interactive mobile customer engagement. The digital world is rapidly changing, and eyes are now on the mobile device as the gateway for that very engagement. Broadly speaking, this engagement may include direct-to-consumer marketing, product information and usage guidelines, personalized loyalty programs, cross-selling of associated brands, consumer feedback and much more.

The third challenge is related to the ease with which products can now move across markets as a result of expanding global supply chains and the dropping of trade barriers. This leads to these questions: *Where exactly are my products? And are they being distributed by my trusted partners?* Recent regulations in some markets for pharmaceutical products have led to the introduction of digital traceability programs. A compelling business case can be made for such a transformation in consumer packaged goods (CPG), durables and many other market sectors to provide similar benefits.

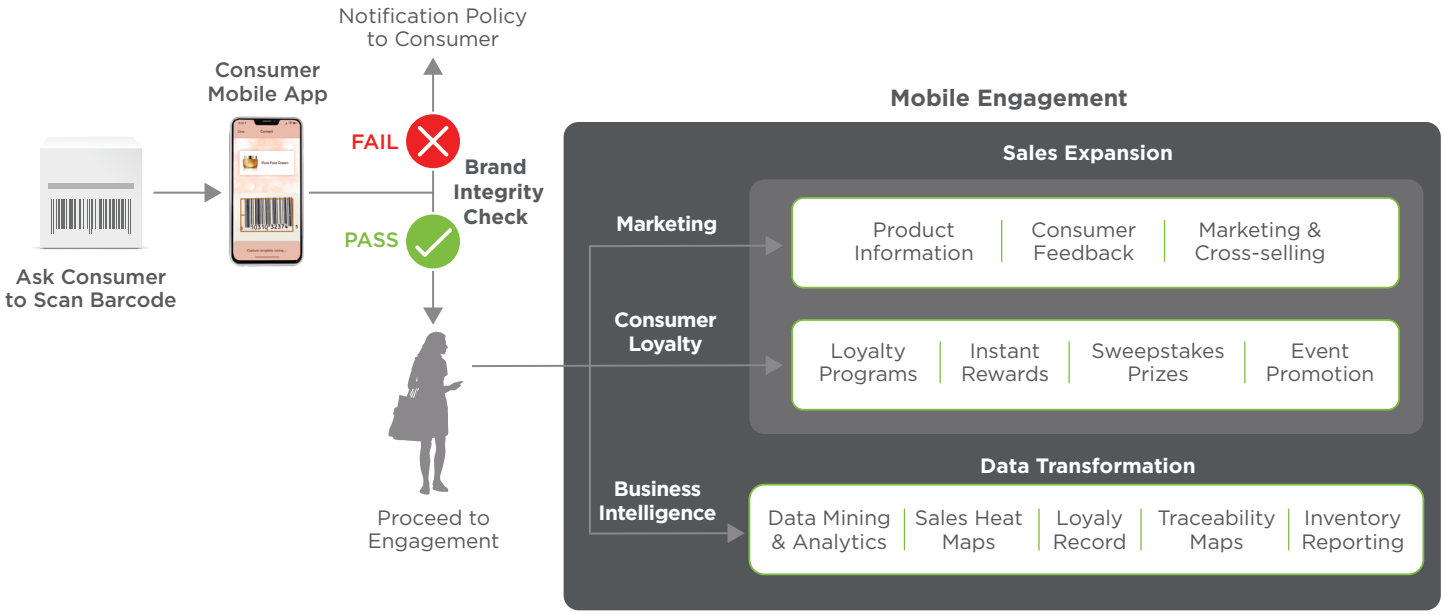
The transformations now taking place in the emerging field of connected packaging can address the above three core requirements—*protection, engagement and traceability*—while delivering powerful supply chain insight. Here, I provide a visionary assessment of what digital conversion to a connected packaging program can achieve if it is well thought out by the brand owner. I also provide a direct exposition of what technologies to avoid and which ones to consider. A compelling case will be made to adopt technologies that can be trusted by virtue of their proven robustness along with the stability and longevity of the solution provider in the global marketplace.

Engagement-driven brand protection

Let's ask a simple, though theoretical, question: How many brand owners are actually prepared to ask their customers to check their purchase and ensure the product is genuine? The question is theoretical because although no formal studies have been carried out, the answer can surely be surmised to be as close to nil as possible. Brand owners will very rarely disclose that their products are under attack.

Rewarding the consumer

One way to circumvent this obstacle is to incentivize consumers to interact with the product because in return they will derive something of value. As the figure below shows, there are numerous engagement options that can be offered to consumers. One is to provide information on the product itself, guidelines on proper usage and even lifestyle advice. The engagement portal can also be used to obtain consumer feedback, sell related brands and even announce a new product launch. All these efforts are aimed at satisfying a basic human desire—the yearning for information and to be in the know on what they consume, what they apply to their bodies and what they keep in their homes. And that in turn can form a very powerful driver for consumers to engage with the brand because they will receive a direct and personal benefit.



Another driver for engagement is the appeal of getting something of monetary value in return for interacting with the product. One common approach is to enlist customers into a loyalty program to drive repeated purchase. Instant rewards can also represent a powerful incentive through cash back directly into the customer's digital wallet. And finally, there is the allure of winning a sweepstake prize. To turn a product into a lottery ticket not only draws customers to that brand but also in turn rewards the owner with increased sales.

The surrogacy model

What do all the foregoing sales augmentation tactics have to do with brand protection? Consider the left side of the figure above. As shown here, the engagement portal would only unfold after the product has been verified as authentic. In other words, the consumer's interaction with the brand first unleashes a check in the background on whether it is authentic. If not, a flag

[1] It would not be the case that the exact identify of a customer is known, nor should it be due to privacy reasons. However, the access credentials to the engagement app would give a login identity that can be used to map purchase patterns and other related insights.

is raised, and the brand owner sends either a warning message or a request for more information. If the product is genuine, as would be the case most of the time, then the interactive portal opens and the brand owner can deliver from a menu of engagement options.

The most important part of this solution is that the consumer is not even aware that a brand integrity check is occurring in the background in the first instance. Consequently, this approach can dramatically increase the number of checks in the marketplace via a large consumer base without disclosing the surrogate nature of the protection program. Consumers are driven to interact with the product because they derive a personal or monetary benefit, all the while creating a multiplicative impact to help curb the menace of counterfeiting and gray market trading.

The BI loop

Each and every consumer interaction with a product in the marketplace furthers the powerful benefit of insight to the brand owner. As shown in the bottom panel of the figure, there is a substantial amount of business intelligence (BI) data that can be mined and analyzed, such as which specific product was scanned, when that interaction took place, at what geographical location and even who the customer is. Regarding the latter, brand owners would gain knowledge on repeated purchases by the same individual, temporal patterns of the purchase and data around the engagement choices to provide insight into customer preferences.[1]

At a macroscopic level, the BI data can be visualized to provide substantial market insight. Sales heat maps, for example, can govern regional sales strategies or discern the impact of localized marketing efforts. The most overt BI benefit however would be the brand protection component. The collective accumulation of adverse events would provide brand owners with actionable intelligence to undertake interdiction efforts, weed out distribution vulnerabilities, fortify oversight efforts or modify defense strategies. The BI component brings the program full circle—clever engagement strategies drive consumer authentication, which in turn amplify brand protection outcomes, that in turn close the loop by giving brand owners coveted supply chain and marketplace data.

[1] It would not be the case that the exact identity of a customer is known, nor should it be due to privacy reasons. However, the access credentials to the engagement app would give a login identity that can be used to map purchase patterns and other related insights.

The switch to digital

How can all of this be done? The older approaches to brand protection involved analog offerings where an overt visual feature such as a hologram, watermark, color shifting ink and other similar solutions represented the mainstay of what was available. None of those solutions however can offer the kind of interactive engagement options described in the previous section. Instead, the current revolution in connected packaging is being driven by digital technologies.

The connected packaging revolution is being driven by digital technologies. Fingerprinting can transform a simple package barcode to meet all core requirements: protection, engagement and traceability.

Serialization – The traditional approach to digitization

An early digital packaging solution involved the placement of a unique serial number on every package, either in human readable form for verification via text messaging, or more recently using a 2D barcode as the carrier to permit authentication via a smartphone app. The original use case for serialized barcoding was to verify the code and therefore presumably the product. The technology was later used to also support an interactive link between the product and its buyer for use in digital marketing, loyalty and other personalized programs.

So why has the world not rushed to deploy serialized packaging in the CPG sector? The most common problem with serial number authentication is that counterfeiters can easily copy a genuine visible code from a genuine package due to its open readability. This is a well-recognized problem with the platform and for this reason product serialization has largely been entrusted for use in tracking programs and not item-level authentication. The possibility that a consumer engagement program with all its marketing promises can be hijacked through serial number replication is most unsettling, and a risk that many brand owners are unprepared to take.[2]

Fingerprinting – The new wave in item-level digitization

The fundamental requirement for brand owners can be stated as follows:

- give them the means to engage with their customers to provide information or reward
- ensure it is executed through a packaging technology that cannot be cloned or reverse-engineered by counterfeiters
- use the reward-information gateway to create a surrogate means for brand protection

and, oh...

- do all this (if possible) without changing or adding anything to the package.

The latter is a highly-coveted requirement not only to contain cost but due to the very fact that brand owners are averse to placing an extra barcode or any additional feature onto the artwork of their perfectly designed package.

[2] A detailed article is available that covers the many reasons why unit-level serialization poses dangers for consumer engagement programs: https://www.securingindustry.com/pharmaceuticals/serialization-isn-t-enough-to-drive-consumer-authentication-says-report/s40/a5790/#.XZIgYy0ZMk8

These requirements represent a very tall order indeed. As it happens, the march of technology has created the good fortune to now provide a solution that meets all these demands. Known generically as fingerprinting, the idea is that a component of the package artwork contains a unique noise pattern that is not discernible to the human eye but can be detected by a smartphone. The key is that no two packages will have the same noise pattern and therefore this fact serves to distinguish each and every individual package.

It is this unseen noise that is authenticated, and which cannot be successfully replicated by a counterfeiter—even if the entirety of the artwork is perfectly copied. Once the noise signal from a package is authenticated, a gateway can then open to engage the consumer. And given that the noise is already an inherent component of the package, nothing needs to be added to the artwork. The solution is fully non-additive with respect to the package and non-intrusive with respect to the deployment. All that remains is to find a way to capture, store and authenticate the noise that is intrinsically present in every package.[3]

A revolution in engagement-driven brand protection

An ideal solution would be one where the linear barcode that is present on all consumer packages provides the locus for the covert noise. This is the exact solution that has been developed by Systech, providing the only offering where a common feature of the package artwork is used in the fingerprinting process.

As shown in the figure above, Systech places a camera and associated devices needed to image the barcode either on the packaging line or at the package supplier location[4]. Once the barcodes are fingerprinted through Systech's platform for a given program they are stored in a secure cloud. The products can then be released into the marketplace where both authentication and engagement activities can unfold via a smartphone application.

This approach offers all the desired requirements as explained above, with the additional key feature that usage of the linear barcode in the program bypasses the need to apply an additional token or taggant on the package. The brand protection program can then be delivered in a surrogate manner through a consumer engagement design.

[3] The noise being referred to here arises as a result of the printing environment where random vibrations in the conversion and handling machinery create a stochastic source of print variability. Combined with various other factors such as environmental dust and other ambient factors, the result is that microscopic imperfections are created in the printed matter. This noise is generically referred to as the fingerprint and is distinct to each package, never being the same regardless of the volume in question.

[4] In this scenario, no additional barcode printing is needed on the package, but only passive image capture of the linear UPC/EAN barcode that is already a part of the package artwork.

Traceability-driven brand protection

Along with brand protection and consumer engagement, there is often the need for one other requirement—supply chain traceability. The current climate of fraud, parallel trading and illegal distribution represents a development that is every bit as disturbing as counterfeiting. This threat reality has led to the growing demand for incorporating a product traceability and anti-diversion program into the brand protection milieu. But here too the same problem arises: how to create a cost-effective program that delivers all the needed benefits without resorting to item-level serialization on consumer goods.

The necessity of package digitization

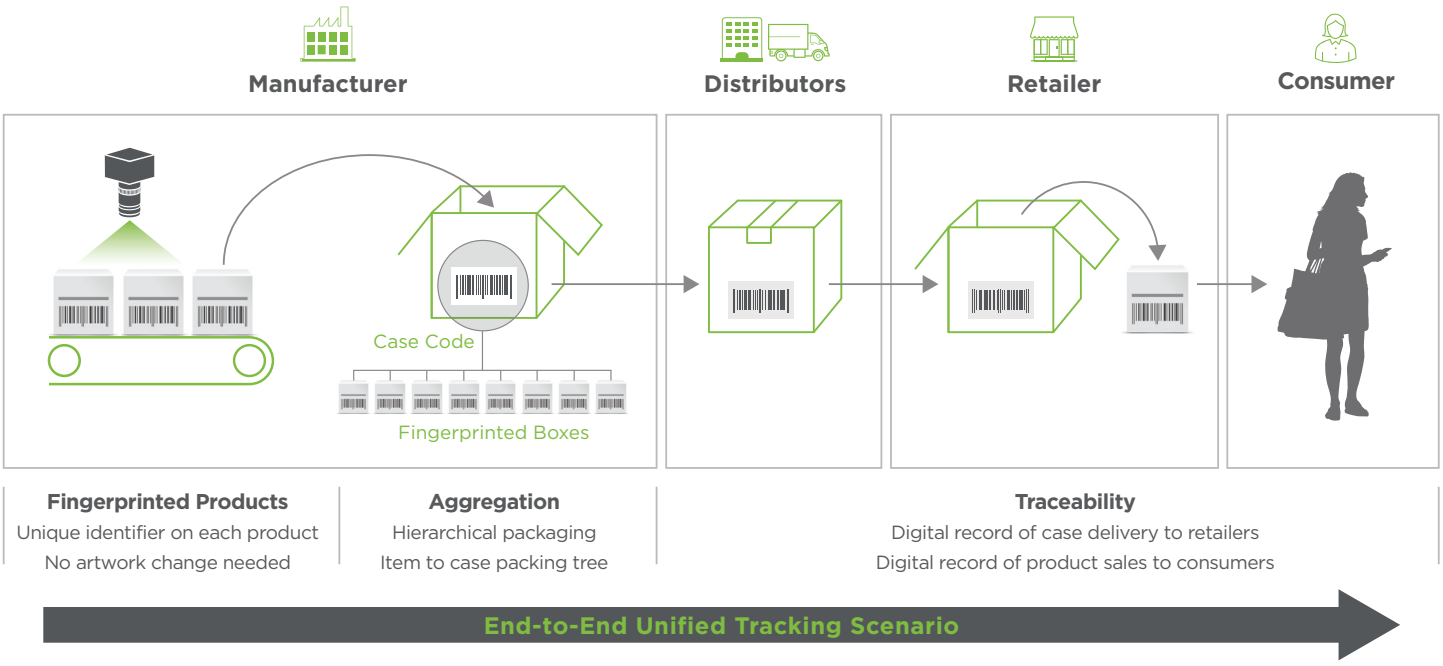
The starting point for all track-and-trace operations is to give a unique digital identity to each primary package and thereafter create a hierarchical tree with all superseding package formats, such as cartons, cases and even pallets. The relevant package levels are then monitored as they move through the supply chain through the rules of inferential tracking. This approach represents the fundamental basis for global traceability programs that have now been successfully deployed in the pharmaceutical industry as mandated for several regulated markets.

When it comes to consumer packages, brand owners are met with an intractable challenge. While the benefits of having real-time knowledge about package movements is well accepted—especially with regard to curbing diversion and illegal trading—it is simply a nightmare to digitize (serialize) at the pack level. Consumer packages come in various shapes, sizes and substrates, all of which make it nearly impossible to institute a variable printing regime on the packaging line. This barrier has represented one of the reasons why item-level traceability programs have not taken off in the CPG sector, despite the well-acknowledged business benefits.

Serialization, without serializing

The advent of fingerprinting technologies expands the possibilities for solution providers to deliver an alternative solution to serialization, as illustrated in the next figure. Given that nearly all consumer packages have a UPC/EAN barcode, the very signal for creating a unique digitized identity for that package resides within that barcode. As explained above, capturing the barcode fingerprint can deliver a unique identity for that package without the need to place a separate serial number or serialized barcode on the pack. The effect of fingerprinting is to serialize at the saleable pack level, without the pain and cost of deploying a variable printing program.

This model has the potential to deliver the remaining aspects of a total traceability program, starting with package aggregation. Here, the connection would not be between serial numbers across different levels but rather between fingerprinted primary products and the next higher package. If that happens to be a shipping case, for example, then the fingerprints are relationally connected to the serial number placed on the case. When that code is tracked, all the included fingerprinted packages are digitally tracked as well. When the case is delivered to a specific distributor, the foreknowledge of all fingerprinted items at that location can be used for the business operation in question. If any of those products show up illegally online, then it would become clearly apparent when the fingerprint is interrogated as to which distributor or retailer had last ownership.



The noise in the marketplace

As the apocryphal Chinese saying goes, *may you live in interesting times*. We seem to have that now with the transition from analog to digital brand protection along with the stunning possibilities of value addition that consumer engagement and product traceability can bring to businesses. And with opportunity comes the prospect for business capitalization. The current brand protection landscape is filled with a multiplicity of providers all portraying the superiority of their solution. How then does a brand owner parse through this noise to arrive at a worthy solution for adoption? There are three elemental but essential guidelines to keep in mind, presented here by way of a summary of the foregoing discussion.

Choose digital

There is no upside to choosing an analog solution nowadays if the objective is to protect brands and consumers with the additional goal of initiating consumer engagement or product traceability operations immediately or as a later calling. Analog solutions of the past, such as holograms, once provided some security value until their own success paved the way to themselves becoming victims of rampant duplication. It is now time to move on and adopt (or convert to) a digital connected packaging solution.

Choose fingerprinting

It would be incorrect to state that all digital solutions are fully safe and therefore immune to replication or hijacking. As discussed before, serialized barcoding is particularly vulnerable to these threats. The emergence of fingerprinting technologies, however, provides exactly the kind of supreme assurance needed in the digital domain because the noise signal in an original package simply cannot be replicated. Consequently, a well-designed fingerprinting program can provide the ultimate in product security, along with the confidence for safe launch of a consumer engagement program in the public marketplace.

Choose experience

The selection of a brand protection solution that combines product authentication with engagement and traceability options must necessarily be a careful and thoughtful exercise due to the high stakes in play. The selection of fingerprinting as the connected packaging solution is an excellent choice. But it is equally important to select a solution provider with an excellent track record of delivering brand protection solutions and therefore can provide the necessary business security assurance that comes through longevity.

Many leading brands across diverse product categories rely on Systech to secure their supply chains. Its brand protection suite provides the only non-additive digital fingerprinting solution based on the linear barcode. Once deployed, Systech provides the most secure platform for an engagement-driven and surrogacy-mediated brand protection program. And with its long pedigree of excellence in traceability deployments across the pharmaceutical industry—one of the world's most heavily regulated markets—Systech brings a level of proven expertise to keep products authentic, safe and connected across the supply chain.

Choosing digital and choosing fingerprinting offers the best option for protecting brands, engaging consumers and tracking products—a perfect trifecta of opportunity delivered through connected packaging. And when it comes to selecting the most trusted provider of these solutions, there is only one answer... choose Systech.

About the author

Avi Chaudhuri, PhD
Chief Scientist, Systech

Dr. Avi Chaudhuri spearheads Systech's brand protection technological development and expansion into the Middle East, India and the Asia Pacific region. In his role, Dr. Chaudhuri is responsible for harnessing and evolving Systech's tech potential to enable customers to fight the ongoing threat of counterfeiting.

Prior to joining Systech, Dr. Chaudhuri designed and deployed serialization, traceability and brand protection programs for some of the largest companies in the world. Additionally, he introduced the concept of mass serialization to the Indian pharmaceutical industry, allowing patients to authenticate their drug purchases via a national SMS program. He has also authored several manuscripts and white papers on technology solutions to combat counterfeiting, which have had significant impact on shaping public policy and protecting consumers.

Dr. Chaudhuri holds a Ph.D. in neuroscience from the University of California, Berkeley. In addition to his work at Systech, he is the founder and trustee of The Purnima Foundation in India.

SYSTECH®

Systech provides digital product authentication and traceability solutions to combat counterfeiting, prevent diversion and meet regulatory compliance. Built on decades of experience as the leader in pharmaceutical serialization, our comprehensive brand protection suite delivers the real-time insight, actionable product data, digital connectivity and consumer engagement functionality needed to fight supply chain threats.

Global brands across industries rely on us to keep their products authentic, safe and connected—from manufacturing to the consumer's hands. Together we are revolutionizing brand protection!

US Headquarters: +1 800 847 7123
UK Office: +44 1482 225118
EU Office: +32 2 467 03 30
India Office: +91 22 4541 1400
China Office: +86 21 51798418

SystechOne.com/UniSecure
Advice@Systechone.com