WHITE PAPER

A Gift to the Counterfeiter: Serialized QR Codes

Avi Chaudhuri, PhD and Jim Lee, Systech International

The emergence of fake barcodes and its implications in the battle against counterfeiting

The Quick Response (QR) code is now everywhere. Invented in 1994, these two-dimensional barcodes have become a common fixture in consumer advertising, appearing in print media from newspapers to billboards. In nearly all cases, these barcodes merely direct the consumer to the product or corporate website after it is scanned. In other words, these are ***static barcodes*** with fixed content and therefore easily printed in a repetitive manner as part of the overall package artwork.

A new trend has begun to appear in recent years — the serialized QR code. By inserting a unique identifier (serial number) into each barcode, brand owners are able to confer uniqueness to their packages at the individual item level. Each product item would therefore have its own unique barcode with a unique serial number. The original goal was to use this uniqueness feature to combat counterfeiting on their brands. If the number is successfully authenticated, the argument went, the same must also be true of the product.

Serialized barcoding has now fallen out of favor as an anti-counterfeiting tool in the CPG industry for various reasons, principally due to implementation difficulties combined with its serious security flaws. A detailed discussion of these problems appeared in a recent white paper.[1] Here, we extend those arguments and provide further insight into how serialized barcodes are now getting hijacked by counterfeiters, drawing on some very recent and troubling incidents that have unfolded in the marketplace.

Although serialized barcoding provides a strong foundation for implementing a traceability program, serious problems can arise if this technology is instead deployed for consumer use. Brand owners who wish to create a consumer-based program — whether to verify product authenticity or use the serialized barcode to drive marketing, loyalty, or other sales augmentation programs — must fully understand the risks at the outset before making the steep investments in such a program.

Common QR code formats

There are two ways that a serialized QR code can be formatted. The first involves placing just a unique serial number into the barcode itself. There is no other content. Scanning the barcode with a publicly available QR code reader would only reveal the serial number, which as shown in the example to the left is useless to a consumer. Solution providers therefore create their own mobile application (app) to be used with such barcodes. The app itself contains a link to the authentication server where the serial number is first verified before the use case is deployed. This arrangement is known as a ***closed-system*** due to the requirement of a dedicated app.

An alternative is to use an ***open-system***, where a link to the server is embedded within the QR code itself, as shown in the example to the left. The advantage to this arrangement is that consumers do not have to download a dedicated app. Both brand owners and solution specialists regard that extra step as a barrier to consumer adoption. Instead, any publicly available barcode reader can be used with this format because the serial number is attached to a link within the QR code itself. Scanning the barcode automatically takes the user to the required servers where the serial number is authenticated.

The security advantage to the first (closed) type is that the link is embedded within a dedicated app and therefore hidden. The drawback however is that counterfeiters try to trick the system by replicating serial numbers from genuine products.[2,3] The solution provider tries to overcome this by limiting the authentication exercise to one instance so that duplicate numbers will raise a flag. The main problem associated with this limitation is its restrictive nature — what happens if a consumer authenticates a product on a shelf but then doesn't buy it?

The advantage to the second (open) format is its ease of use due to the fact that any publicly available QR code reader can be used. However, an entirely different problem now arises with alarming frequency in the global marketplace. This problem, which we refer to as ***phantom barcoding***, can actually target both the open and closed types of serialized barcodes, as discussed in the next section.

Fake Barcodes and phantom links — Implications for the brand owner

The greatest threat from use of QR codes arises from the very nature of their design — they were created for machine readability and not for human visual analysis. The arrangement of the elements encodes the data through an algorithm that is undecipherable to the human eye.[4]

Another vulnerability arises from the open nature of the QR platform itself. Anyone can easily replicate any QR code, incorporate any information they want, and place it on a fake product to make it appear nearly indistinguishable from that on an original product. And that is precisely what is starting to take place.[5]

A recent wave of incidents highlights the ease with which a fake website can be inserted into a barcode and placed on a product. Consumers are then misled with false information or tricked into providing their banking details or coaxed into divulging personal data. In recent incidents, fraudulent QR codes were used to steal millions of dollars from consumers in China[6] and Malaysia.[7] The widespread use of digital wallets such as WeChat Pay and Alipay that use QR codes have only compounded the problem.

It is believed that this problem will quickly spread to consumer products if serialized barcodes should make their way onto the packaging, where the exact same technology (QR) and principles (fake website) can be deployed with ease.[8,9] Criminals who have made major investments in their counterfeiting program are not easily deterred and therefore will make every attempt to replicate the security technology as well.

Consider the following scenario. A major brand adopts a serialized QR coding program as a brand protection initiative. Given that the counterfeiter has already replicated the package to near perfection, he now merely inserts a fake QR code into his artwork that points to his own server. The two barcodes are nearly indistinguishable; see the example where the one on the left points to a genuine website and one on the right to a fake one. Unless the brand owner deploys a massive marketing program to educate consumers, the default practice will be for a customer to simply scan the barcode on the fake product only to be reassured that it is genuine. The emergence of QR code readers on social media apps and new Smartphone models makes this deception that much easier to unfold.

Risk mitigation and possible solutions

The threat from phantom barcoding is very real and adverse events are already unfolding. One option is for brand owners to make clear to consumers that they need to be vigilant and examine the website after a barcode is scanned.[10] Brand owners must therefore divulge that a counterfeiting problem exists and then place the burden on the consumer, which few are willing to do.

A more preferred risk mitigation approach is to deploy tactics that directly reduce the threat and protect the consumer. A few options are given below in order of increasing effectiveness.

Hide the serialized barcode

A few companies have opted to use serialized barcodes as part of their loyalty and sales augmentation program.[11,12] The barcodes are placed inside the package to prevent redemption without purchase. While this approach serves the goals of a loyalty program, it would not represent a consumer-friendly approach to brand protection. If a counterfeit product is discovered prior to purchase, then the consumer has a reasonable recourse. If it occurs at any point thereafter, then the consumer is burdened with the task of a return visit to the store or absorbing the loss. These are not very good outcomes and never to the benefit of the brand owner because of reduction in consumer confidence and dilution of brand equity.

Protect the barcode with another technology

A number of innovative technologies have recently appeared that serve as an additional layer to protect the barcode itself. These are generally proprietary offerings that secure the barcode via a closed system through a dedicated mobile app. Although these applications can be effective with proper consumer education, the fundamental flaw in this approach arises from consumer vulnerability of being duped by a fake barcode to begin with. This issue is similar to the now familiar problems with counterfeit holograms — they can look perfectly like an original but are indeed fake. Similarly, a falsified QR code on a counterfeit product can easily deceive consumers, leading them to simply scan that barcode with a public-domain app. No amount of layering will protect against deception through substitution in the face of unawareness.

Restrict serialized barcode use to brand promotion (activation) campaigns

As noted above, serialized QR codes can be used to drive loyalty and gamefication campaigns to boost sales. An argument can be made that a restriction to this use alone could validate the use of mass serialization. This position is tenable so long as two factors are strictly met — the brand itself is not susceptible to counterfeiting and the market it is sold in is generally exempt from criminal tampering activities. The global spread of counterfeit products, especially through the rapid rise of eCommerce, makes both of these conditions uncertain even in the most immune markets. Whatever the source of the problem, the brand owner's loyalty and CRM program can be just as easily hijacked, leading to possible PR disasters.

Deploy a third-generation solution

The recent advent of third-generation (3G) solutions has ushered in a new era in the fight against counterfeit products.[13] A 3G solution is one that can neither be successfully copied nor emulated. A few technologies can lay claim to this strict requirement. The two leading offerings include NFC tags[14] and fingerprinting technologies.[15,16] Systech's UniSecure® fingerprinting solution has drawn special acclaim because it is based on the printed linear barcode found on nearly all packaging, making it the only non-additive technology in the marketplace. Furthermore, these barcodes cannot incorporate website addresses and therefore the phantom barcoding problem simply cannot arise. In addition to providing a robust security platform, UniSecure enables a full complement of consumer engagement and brand activation programs.

Summary

Counterfeiters practice their craft when two conditions are ideally met — they can do it easily and they can get away with it. These conditions are best found in Asian markets where the ubiquitous presence of QR codes combined with laxity in interdiction makes for an ideal environment.

Prior concerns with mass serialization related to the ease of copying a genuine number from a genuine product and then reproducing it on fake products.[17,18] The recent emergence of outright hijacking of QR codes in Asia represents an entirely new dimension to this problem, and one that is far more insidious. A number of factors come together to create the perfect storm — the inability of consumers to differentiate fake from genuine barcodes, the ease with which consumers can then be directed to a fake website, and the challenge that brand owners face in undertaking a large and sensitive campaign on consumer vigilance.

In short, it has become very easy for the counterfeiter to falsify a serialized product, regardless of whether it is implemented via an open or closed system. And hence the provocative title of this article — serialized QR codes really are a gift to the counterfeiter and an open invitation to go at it.

About the authors

Avi Chaudhuri, PhD
Senior Global Partner, Systech International

Dr. Avi Chaudhuri has over twelve years of experience in the field of brand and consumer protection against counterfeit products. He is currently responsible for spearheading Systech's expansion in Asia, with focus on the UniSecure platform as a third-generation brand protection and consumer engagement technology. Dr. Chaudhuri introduced the very concept of mass serialization to the Indian pharmaceutical industry in 2007 and helped to create a national SMS program for drug verification.

Jim Lee
Senior Vice President, Product Management, Systech International

Mr. Jim Lee has an exceptional background in Product Management with over 25 years of broad industry experience delivering numerous new products and creating new product categories. In his current position at Systech, Mr. Lee is responsible for Product Portfolio designed to deliver market-leading brand protection, anti-counterfeiting and product identity solutions.

References

[1] Chaudhuri, A., Lee, J. (2017) Serialization Reality Check: Where are all the Numbers? The failure of serialization-based technologies to drive brand protection, customer loyalty, and consumer engagement in the CPG sector. A Systech White Paper. http://www.systechone.com/wp-content/uploads/systech_serializationrealitycheck.pdf

[2] Counterfeit Products. Bose Alert (2018) https://www.bose.ca/en_ca/legal/be_aware_of_counterfeit_products.html

[3] Government bans mobile phones with duplicate, fake duplicate identity numbers (2015). The Economic Times (India). https://economictimes.indiatimes.com/industry/telecom/government-bans-mobile-handsets-with-fake-duplicate-identity-numbers/articleshow/45944630.cms

[4] How secure is a QR code? (2017). http://qrcode.meetheed.com/question10.php

[5] QR codes too easily misused by criminals (2017). China Daily. http://www.chinadaily.com.cn/opinion/2017-03/02/content_28400890.htm

[6] Yezi, L. (2017) Scan no scam: Police arrest two fraudsters for cheating via fake QR codes. https://news.cgtn.com/news/3d45444d7959444e/share_p.html

[7] Watch out for fake QR codes, warns IT security provider (2018). http://www.freemalaysiatoday.com/category/nation/2018/02/01/watch-out-for-fake-qr-codes-warns-it-security-provider/

[8] Kostur, P. (2016) Let's fake it — How to crack a unique QR code & serial number. https://www.linkedin.com/pulse/lets-fake-2-how-crack-unique-qr-code-serial-number-peter-kostur/

[9] Fighting brand piracy using QR codes (2011). https://qrworld.wordpress.com/2011/10/10/fighting-brand-piracy-using-qr-codes/

[10] O'Donnell, A. (2017) How to protect yourself from malicious QR codes. https://www.lifewire.com/how-to-protect-yourself-from-malicious-qr-codes-2487772

[11] Pampers diaper rewards program. https://www.pampers.ca/en-ca/rewards

[12] Tode, C. (2018) Danone links QR codes with loyalty program to drive savings. https://www.mobilemarketer.com/ex/mobilemarketer/cms/news/database-crm/15706.html

[13] Chaudhuri, A., Lee, J. (2017) The Evolution of Brand Protection: The emergence of a new generation and a unique new technology. A Systech White Paper http://www.systechone.com/wp-content/uploads/the-evolution-of-brand-protection-jun-2017.pdf

[14] QR codes and anti-counterfeiting: The false sense of consumer security and why NFC is the most appealing alternative (2018). https://selinko.com/blog/qr-codes-and-anti-counterfeiting/

[15] Arjo Solutions launches Safe app for authentication based on Signoptic technology (2016). http://www.labelsandlabeling.com/news/new-products/arjo-solutions-launches-safe-app-authentication-based-signoptic-technology

[16] Systech launches UniSecure™: The ultimate anti-counterfeiting tool (2015). https://www.businesswire.com/news/home/20150928006053/en/Systech-International-Launches-UniSecure™

[17] Manning, M. (2018) Viewpoint: Are you gambling with 2D data codes? https://www.securingindustry.com/pharmaceuticals/viewpoint-are-you-gambling-with-2d-data-codes-/s40/a7096/#.WqFY-ebrtag

[18] Mass serialization 'failing' in consumer products sector [2017). https://www.securingindustry.com/mass-serialization-failing-in-consumer-products-sector/s112/a3127/

SYSTECH®

Systech is the global technology leader in supply chain security and product authentication. For more than 30 years, we have put technology on the line. Systech pioneered pharmaceutical serialization as well as innovations in line vision and inspection, overall packaging line management and track and trace.

Today, Systech is revolutionizing brand protection. Our software solutions ensure products are authentic, safe and connected—from manufacturing to the consumer's hands.

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
Sales@SystechOne.com