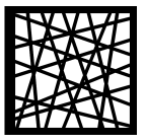
The Weaponization of QR-Codes and the Impact on Brand Protection

An iTRACE Technologies, Inc. White Paper

iTRACE Technologies, Inc
3790 El Camino Real Unit #644
Palo Alto, CA 94306
USA
+1-650-241-1958
www.itracetech.com



Executive Summary

In February of 2025 the Google Threat Intelligence Group (GTIG) released a white paper titled Signals of Trouble. This article highlighted how Russia was weaponizing the QR-Code on popular messaging apps to gain access to systems, data and devices. Hidden in the article were descriptions of attacks that extended beyond the messaging apps to other techniques and tradecraft targeting everyday systems using QR-Codes. These malicious QR-Codes can steal credentials, download malware and gain access to devices and business systems.

This White Paper explores the threats to anyone deploying QR-Codes in their business processes with a particular focus on the current trends in brand protection to use QR-Codes as a track and trace solution for products. This is especially relevant to the deployment of the Digital Product Passport in Europe and the Sunrise 2027 initiative from GS1 in the USA. As the use of QR-Codes becomes more prevalent and required by some regulation, the attack surface affecting brands and their customers will grow exponentially. Adding holograms and pixie dust around the QR-Code will do almost nothing to thwart these attacks and only highlights how weak the typical brand protection application is when deploying a QR-Code as the data carrier combined with virtually any other technology.

The perceived balance of convenience vs security has swung too far to the convenience side of the scale to the point where there is little to no actual security in the vast majority of today's anti-counterfeit implementations. There are many documented instances of QR-Code solutions being exploited and causing harm to consumers and brands, some of these have been included in this White Paper along with the many warnings from various organizations including the FBI and US FTC regarding the dangers of scanning QR-Codes. We have tried to highlight these issues as well as the current recommendation to mitigate the risk. We look at the alternative solutions that will need to be explored to help brands actually take the fight to the counterfeiters, because today the numbers show the brands are clearly losing the battle against counterfeiters on all fronts. Using weak solutions incorporating QR-Codes may be costing more as they're paying for a solution that doesn't work and still losing business to the counterfeiters.

About the Author

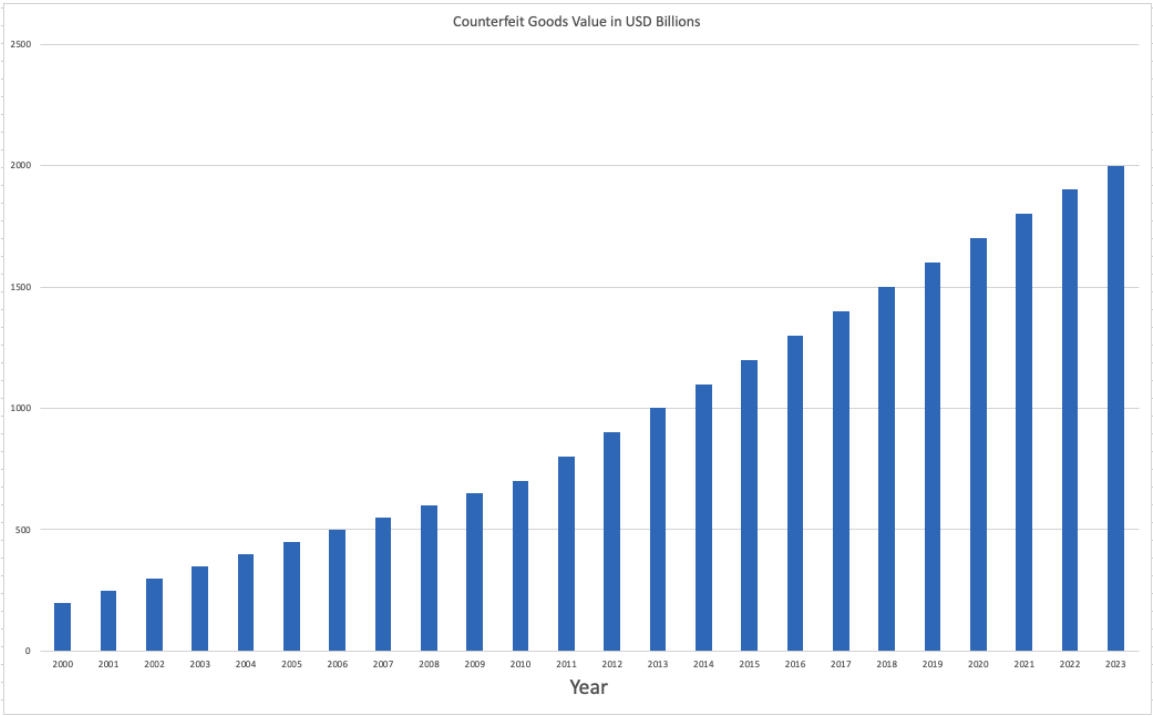
Mark Manning is the Founder and CEO of iTRACE Technologies, Inc. (www.itracetech.com), a leading provider of unique identifier (UID) solutions for manufacturers and brands with customers in Aerospace, Automotive, Medical Device, Consumer Electronics, Fashion Accessories and the Diamond industry.

Mark has over 20 years' experience in brand protection and supply chain security and has worked in technology focused industries for over 30 years including Cyber Security. Mark has also been a brand owner as the Co-Founder and COO of DODOcase Inc, a San Francisco manufacturer of hand-crafted cases for Apple's iPad. DODOcase experienced first-hand the impact of fake products and Mark has personally experienced the damage that fake products can do to a brand and its business.

The Brands are Losing the Battle

We recently performed an analysis of the published value of counterfeit good in US Dollars from the year 2000 up to 2023. What we found was regardless of where we looked, the value of counterfeit goods had only ever gone up, in no single year had there been a downturn.

The brands and brand protection solution providers are losing the battle against the counterfeiters 23 – 0 by this score.



Having been attending brand protection industry conferences since 2004 it clear that the basic reasons that the brands are losing are as follows:

- The counterfeiters are way better at using today's technology than many brands.
- They're smarter and better resourced than you think.
- They're highly motivated by the profit from their activities

- Unlike the brands they don't follow laws, regulations, worry about budgets, re-orgs or holidays.

The Uses for QR-Codes in Businesses

QR-Codes are everywhere today, they're being included into business processes and used as engagement tools everywhere you look. Here are just some of the thing's organizations are doing with QR-Codes today outside of the general marketing engagement and call to action.

- Product Authentication
- Consumer Engagement
- Digital Product Passport in Europe
- Sunrise 2027 in the USA
- Banking Device Enrollment
- Fin Services QR sign-in
- Fin Services QR payments
- Parking Meters and Parking Payment Kiosks
- Restaurant Menus
- Ride Share Bicycles

Why do Organizations use QR-Codes?

Here are some of the most common reasons that companies use QR-Codes today:

- QR-Codes do not require an app download to read with smartphones
- QR-Codes can be scanned by almost every supply chain scanner
- They're free to print, read and are easily recognized by the user
- They can create automated actions with devices and reduce friction for activities
- In many cases they're required by regulation like DPP

But!... Nation States have Weaponized the QR-Code

In February of 2025 the Google Threat Intelligence Group (GTIG – Google's Cloud Cyber Security Arm) released a white paper titled Signals of Trouble. This article highlighted how Russia was weaponizing the QR-Code on popular messaging apps to gain access to systems, data and devices. Hidden in the article were descriptions of attacks that extended beyond the messaging apps to other techniques and tradecraft targeting everyday systems using QR-Codes. These malicious QR-Codes can steal credentials, download malware and gain access to devices and business systems connected to those who scan them. These kinds of attacks are typically

labeled as Quishing and QR-Jacking and Russia is not the only ones using them. Quishing and QR-Jacking attacks are popping up everywhere around the World where QR-Codes are being used.

Quishing or QR Phishing

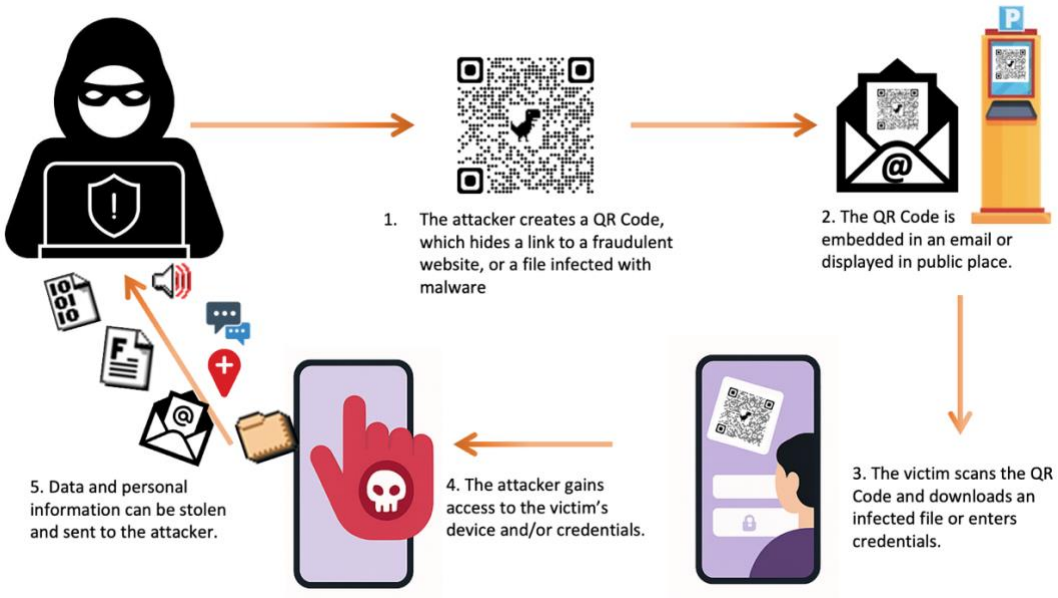
Quishing refers to the use of QR-Codes in phishing attacks that are targeted to steal the credentials or personal information including passwords, personal information, payment and credit card information from people scanning the malicious QR-Code. The QR-Code can be sent to a user in an email, letter and even packages with a message that persuades the user to scan the code.

QR-Jacking

QR-Jacking is generally referred to as the act of hijacking a legitimate QR-Code and replacing it with a malicious QR-Code that will perform the same task as the original with different results for the user. Think about replacing the QR-Code on a ride share bicycle or parking meter causes the user to make the payment to a different account than intended.

Both attacks have very similar characteristics, a legitimate QR-Code is replaced with a malicious QR-Code that will perform hidden or obscured actions to deploy malware, steal credentials, payment or credit card information and generally abuse business logic.

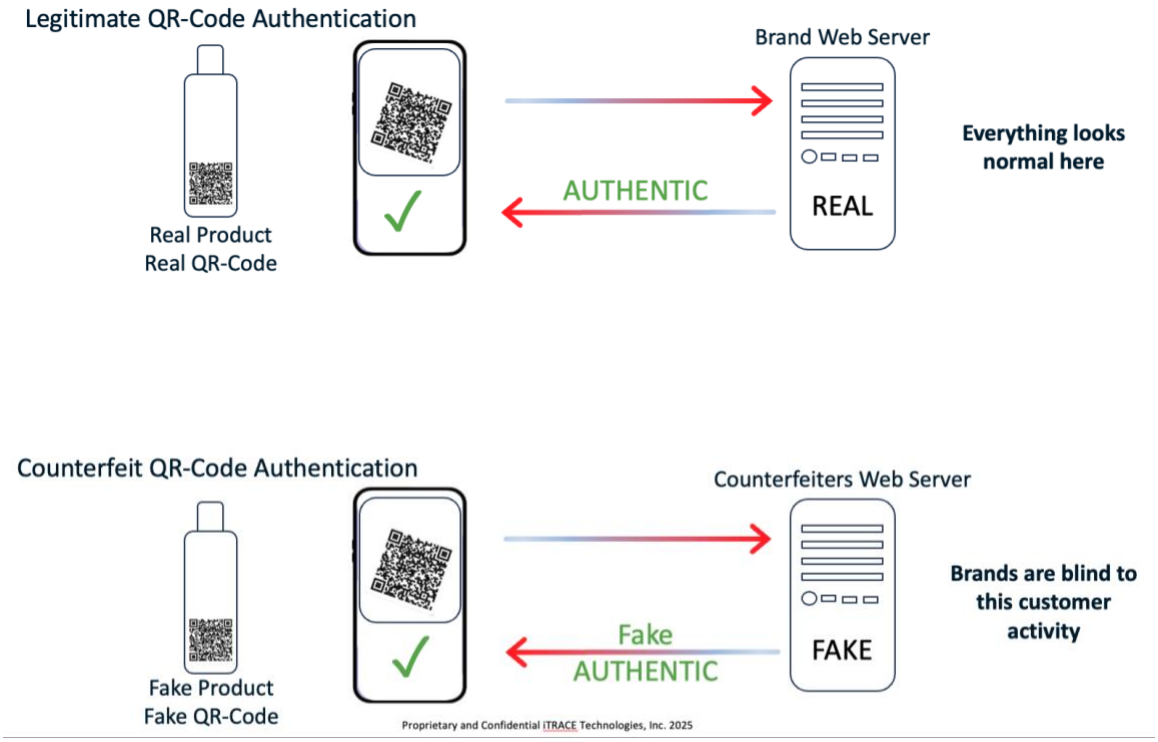
What is Quishing & QR-Jacking



How does QR-Jacking Work in Brand Protection

When a brand deploys a QR-Code based solution as part of their brand protection solution it actually becomes a gift to the counterfeiters, the QR code will be useless in protecting consumers and instead actually cause further harm.

In the top half of the image, a QR-Code is applied to a legitimate product and generates an authentic response when scanned by the user's mobile device. But in the bottom half of the image, a fake product has been labeled with the counterfeiter's own version of the QR-Code that takes the user to a totally fake authentication experience. The brand and their service provider will never see these fake scans and to their systems there will appear to be no counterfeits. Their anti-counterfeit solution provider will appear to be doing a grand job of protecting their product.

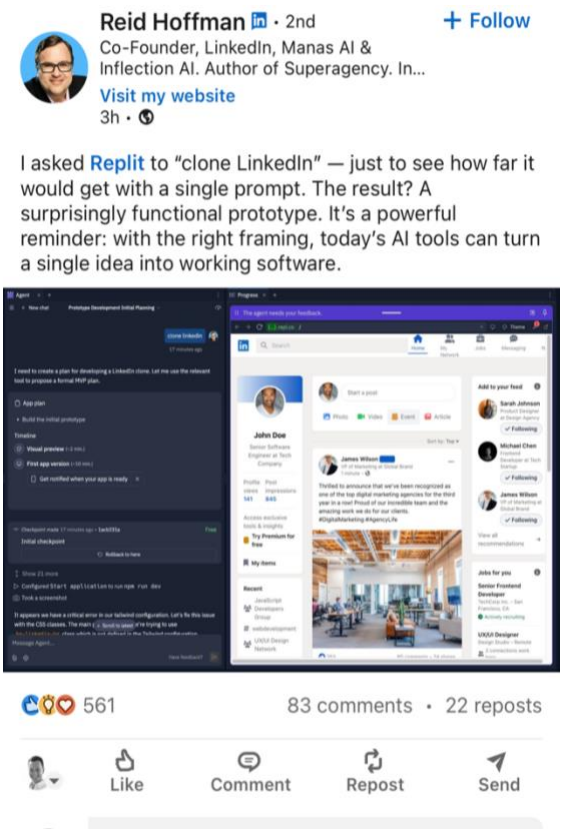


If a product has a QR-Code on it as the data carrier then it will be easy for the counterfeiters to "Clone" the whole authentication experience. The legitimate system will never see these counterfeits and will provide no protection to the consumers.

AI is Automating this Process

Deloitte predicts that losses from AI-driven fraud could exceed $40billion within the next three years, an increase of $12.3 billion since 2023.

Reid Hoffman (LinkedIn Co-Founder) posted on April 17th 2025 that he had cloned LinkedIn with a one-line prompt into Replit. How much effort do you think it's going to take for counterfeiters to clone an authentication experience with their own QR-Codes as the authentication tool?



Don't Scan QR-Codes

There is no shortage of warnings about these kinds of attacks, multiple warnings have been issued by the FBI, US FTC, the US Army, many Cyber Security companies and even Which Magazine has put out articles warning people against scanning QR-Codes.

In the list of the Seven Cyber Security Commandments, the number one commandment is:

1. Stop scanning QR-Codes. QR codes are the Trojan horses of modern convenience. A simple scan can redirect you to a malicious site, steal your credentials, or install malware on your device. Why trust a code you can't read with your own eyes? It's time to think before you scan.."

Yet, even with all of these warnings and cases of QR-Code abuse, regulators, vendors, organizations and brands are still trying to deploy QR-Code based solutions for track, trace and authentication of products. Although this is not a new attack vector, the proliferation of QR-Codes means that the opportunities to deploy these attacks has grown exponentially in recent years, especially in the post pandemic contactless world.

The first malicious QR-Code was discovered in 2011 by Kaspersky labs in Russia. When the malicious QR-Code was scanned by a user with an Android device, it would deploy a Trojan via a

fake version of an app. The app installed malware that forced their device to send texts to a premium service, costing victims $6 per message.

These are not Theoretical Attacks

Here are some real-world examples:

*AMD Ryzen – QR-Code heatsink markings were reproduced and applied to non-functioning Intel chips which were put back in their original boxes. A new QR-Code sticker with a hologram was created for the outside of the box that generated a fake authentication response. The original and genuine items were sold unboxed on e-bay to crypto currency mining operations.

**ING Bank in the Netherlands. Their app allows customers to log into a second device by scanning a QR code shown in their mobile app. Cybercriminals identified this feature as an opportunity to hijack ING clients' accounts by tampering with legitimate QR codes within the app. After falling victim to the scam, unsuspecting users quickly discovered that thousands of euros had vanished from their accounts.

Quishing poses a greater threat when focused on extracting banking and payment details. In a case from ***Texas, cybercriminals attached fake QR code stickers to pay-to-park kiosks, making drivers believe that they could use them to pay for parking. By scanning the codes, drivers were directed to a site where they would enter their credit card information, unintentionally providing their confidential data to hackers.

Something similar happened in February 2022 in ****Atlanta, as drivers discovered fake parking tickets featuring QR codes on their vehicles, supposedly for fine payment. After becoming aware of the situation, local authorities warned that Atlanta does not use QR codes on their parking tickets.

* https://www.pcmag.com/news/fake-amd-ryzen-chips-appear-for-sale-on-amazonebay
** https://www.securitymagazine.com/articles/97949-qr-code-phishing-scams-target-users-and-enterprise-organizations
*** https://www.govtech.com/security/beware-of-quishing-criminals-use-qr-codes-to-steal-data
**** https://www.atlantanewsfirst.com/2022/02/04/beware-fake-parking-ticket-scam-targets-atlanta-drivers/

India's Drug QR-Coding Debacle

Indian Ministry of Health and Family Welfare issued a mandate in 2023 requiring the top 300 drug brands to print a QR code that when scanned by consumers would provide key information such as the brand name, manufacturer details, batch number, and expiry date. This QR-Code was also used to provide a mobile app authentication for the doctors and patients and many proclaimed that there would be no more counterfeits. It is obvious now that the QR-Code that

was meant to protect consumers has been compromised and copied or reproduced versions are now being found on counterfeit products.

Professor Avi Chaudhuri, former Chief Scientist for Systech International, has been in India investigating this issue, he has been shocked at how widespread this counterfeit issue is and how easily it is to get the Indian system to return an authentic response to a fake product. In a series of case studies, Professor Chaudhuri describes all of the attacks on this simple system and how the program is not fit for purpose in its current form.

In a quote from the case studies ** “The Indian anti-counterfeiting program meant to protect domestic drug supplies has failed, and is actually now a gift to the counterfeiters” the article continues “It has now emerged that the very QR code meant to protect Indian consumers has itself been compromised through copied versions appearing on fake medicines. This is not the least bit surprising because it is expected that counterfeiters will use every means to try to defeat a new product security system. What is surprising however is how easy it is to trick the Indian program to actually prevent counterfeit detection.”

** https://www.securingindustry.com/pharmaceuticals/india-s-drug-qr-coding-programme-anatomy-of-a-debacle/s40/a16877/

These are just a few examples of where the current QR-Code solutions are failing brand owners and users, unfortunately most label and packaging printers are not sophisticated enough to provide more effective solutions, the unsuspecting client gets sold just what they ask for, not what works to solve their problem.

The Restaurant Menu Attack

The Restaurant Menu Attack is the last example which is more of a warning to all users about the risks of scanning QR-Codes in everyday places. In an article labeled Step Away From the QR Code and Read These 7 Safety Tips By Len Noe. Tech Evangelist and White Hat Hacker, Len Noe shows how Restaurant menus that use QR-Codes can take users to malicious sites that mimic the restaurant menu but are designed to steal a user’s personal information or payment data.

The article highlights how there is no way for a human to read the QR-Code on the menu and determine if it is malicious or not. If they’re really paying attention the user may notice a different URL once the code has been scanned but that is often too late.

The big problem here is that humans cannot read QR-Codes.

The Attack on the Brand Itself

Isn't Quishing just a customer problem, what's the impact to the brand? It doesn't take much imagination to see how a brands own QR-Codes could be weaponized against them. Let's imagine for a moment that an adversary wanted to gain access to a brands own systems, it would be easy for them to create a malicious QR-Code on a genuine or fake product and send it to a brand representative with a note that said, "hey, is this item real? I can't get it to scan." The representative would likely scan the QR-Code for themselves and open their device to malware that could steal passwords or other data. I'm sure the brands IT team or Cyber Security team are busy training their staff to be careful but this is their own QR-Code right? Who would suspect that?

It's the Users Problem

When these issues were discussed with representatives from GS-1 the response was "Consumers and businesses everywhere should practice digital safety when operating any technology - QR codes are no exception."

"The QR Codes powered by GS1 Digital Link do not pose significant risks to consumers who follow digital safety practices"

They suggest that it's the user's problem and there is no significant risk if you follow digital safety practices, conversely if you don't follow these digital safety practices then there will be significant risk to the user from the GS1 system. What are these digital safety practices that GS1 are recommending? They don't say but the most common recommendation is "Don't Scan QR-Codes".

The industry seems to be adopting the stance that it's not their problem with the most common recommendations requiring Education, Abstinence and asking people to be careful. We have to do better than that.

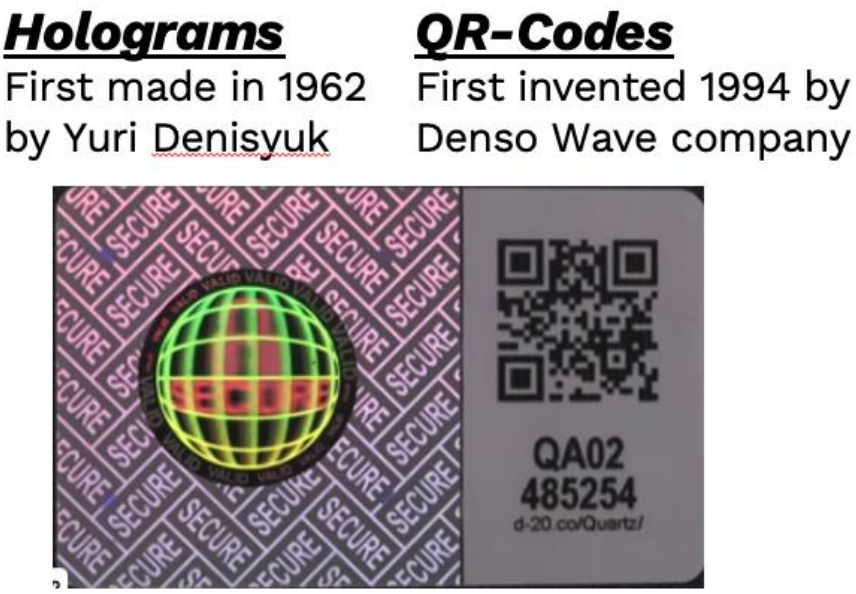
The Industry That's Still Using 1980's and 1990's Tech

The first hologram was made in 1962 by Yuri Denisyuk and fundamentally they haven't changed much since, there are 1000's of companies around the world that can create a passable replica of the OVD's being used in brand protection. Even the team at Kurz Scribos, a leading provider of hologram foil, have publicly stated that holograms are easy to copy. A large US footwear company attending the 2024 IACC conference in Orlando said "Our Hologram is just for decoration; it doesn't provide any security" and they are using technology provided by one of the premium hologram providers in the world. Holograms look fun but they have significant

limitations when it comes to their use for authentication of products and packaging. That's an expensive decoration for a QR-Code

The QR-Code was invented in 1994 by the Denso Wave company in Japan. Its original intent was as a logistics tool to allow parts to move easily through a factory production environment. It was never meant to be a security solution and its open-source nature means that it can be created and read by anyone with the commercially available software and a printer. The problems really started when mobile devices started to natively read QR-Codes and act on the information within them, the scanning of QR-Codes exploded during the global pandemic where everyone started using them for more than just the traditional marketing and engagement.

The Modern Security Label



The industry has pushed forward with these technologies by combining them into one label in the hope that one old technology can fix another old technology. In reality this just creates an expensive label that is still easy for counterfeiters to reproduce at scale, in a way that is very difficult for the brand to detect and likely impossible for the user to identify.

This is not the way that we can drive down the problem of counterfeit, the industry needs new technologies that significantly raise the bar against attack and provide a significant barrier to counterfeiters.

Holograms and Pixie Dust Won't Help

It also doesn't matter what you sprinkle around the QR-Code to try and protect it, a mobile device will act on a QR-Code and only the most experienced or trained user will notice the difference. That's not a theoretical attack, it's happening to brands today and will only get worse.

Holograms are no longer an authentication tool, its well understood that holograms are easily replicated so as only the most experienced or trained investigators will be able to tell the difference. That's no help to the grandma trying to check her medications or college kid authenticating sneakers.

Looking Forward

Forward thinking organizations are actively seeking non QR-Code solutions to secure their products and supply chains. Vendors are looking to deliver new and cutting-edge technologies to their clients. These include technologies that are non-cloneable, digital solutions that can be used on products and packaging to deliver secure mobile device authentication without the need to download a specialized app.

In the next generation of technologies clones and copies can be defined as different attacks on the supply chain. A technology needs to be able to defend against both to be successful in the long run.

Clones vs Copies

iTRACE defines clones and copies in the following way to differentiate the distinct differences in the attack vector from the counterfeiters. Every solution should start with securing the factory or OEM to ensure compliance with production orders and preventing clones, production overrun or 3rd shift activities.

Clones: Reproduction of security markers from the original source files through reproduction or repeat printing. Likely an inside job with hacked systems or production overrun for loose integrations.

Copies: Reproduction of security marks from previously printed or applied marks on products through photocopying or scan and print.

Having a solution that can detect clones and copies is important to ensure a secure supply chain and enable effective product authentication for everyone that touches the product.

Blockchain is not Magic

Due to its close connection with the crypto currency industry, there are many myths around the capabilities of Blockchain to solve the worlds counterfeit problems. These myths are typically spread by organizations trying to make a quick buck by dazzling organizations with the hot new technology and feeding off the hype around these crypto technologies. Blockchain by itself cannot prevent or solve the counterfeit problem, to be effective a Blockchain needs to maintain a secure connect between the physical item and its digital twin, just like any database. As we've described in this article this connection cannot be maintained by a QR-Code and a Hologram.

The next generation of technologies need to be non-cloneable, and provide the secure connection between the product and any digital ledger link Blockchain or other database.

What Happens When the Packaging is Gone

Most anti-counterfeit solutions are delivered through labels or printed packaging, so how do you authenticate a product when the packaging is long gone? If a consumable item has been installed in a machine and the machine fails because the consumable was fake, how do you tell? Brands are now adopting layered solutions that have authentication on both the product and packaging. Having a technology that can be applied directly to parts as well as the packaging allows a seamless integration at all levels of the supply chain and supports the authentication of parts for warranty repair and replacement. Many label and package based solutions are just not capable of being applied directly to the product in this way requiring multiple different technologies or a compromise of only one layer or security. The fight against the counterfeits really needs to be made at all levels of the product to be most effective and provide a long-term solution for the circular economy.

Conclusion

The way that counterfeiters are using today's technologies including AI is many steps ahead of the brands that are trying to defend their products against them. The current QR-Code and Hologram based solutions being delivered by the industry are just not effective against todays well-funded, well-resourced and highly motivated counterfeiters. Counterfeiting is big business and the counterfeiters are not going to give up just because they have to apply a hologram, print a QR-Code and create a fake website. All of that work is well within the margin of the sale of fake products.

If we are going to have any significant impact on the volume of counterfeit goods our entire industry needs to up its game and deliver solutions that are more secure, non-cloneable, const effective and can be applied to the actual product as well as the label or package.

By using the current QR-Code based solutions the brand is typically losing twice. They're paying for a solution that is largely ineffective and they're still losing business and brand value to the counterfeiters. That's aside from exposing their business and clients to the risks of Quishing and QR-Jacking.

About iTRACE Technologies, Inc.

iTRACE has patented an ultra-secure, non-cloneable and cost-effective solution called iTRACE 2DMI® that can validate the authenticity and integrity of products throughout the track-and-trace process without the need for an app download. Our UIDs can be applied overtly, or covertly, onto any solid surface: large or small, rough or shiny, part or package. Therefore, iTRACE 2DMI® is an ideal solution for manufacturers that need to integrate or retrofit UIDs into established products and complex manufacturing environments. Additionally, smart devices with a low-cost camera or sensor can easily be configured to read iTRACE 2DMI® codes.

iTRACE Technologies, Inc., is headquartered in the heart of California's Silicon Valley with a wholly owned subsidiary in Ireland.