Counterfeiting is a big problem

around $1.6 trillion as of today. There are a handful of partial solutions available, but none is really solving the core problem.

The solution to address the largest segment of merchandise counterfeited (ranging from $20 to $1000) need to be foolproof, and cost effective. The typical solutions offered today are holograms, rfid based tags, random 2D graph, scratchable QR codes, and Digital number based SMS system.

We found that every partial solution offered today to address counterfeiting can be counterfeited, meaning the tags or the scheme they employ can be copied and replicated easily. Below are our findings and rough estimate on how much it costs a counterfeiter to replicate and fool the solution provided.

Let’s explore each solution one by one:

Holograms Tags/Labels/Stickers

All it takes to copy the hologram is, give one of the original to the hologram printer company and it will give you exact copies of it. It will even cost less to the Counterfeiter to get the exact Tags/Labels/Stickers from any hologram printing lab near him. Usually the price ranges from less than 1¢ to 50¢ depending on the complexity, colors, layers, materials, and size involved.

Random 2D Graph stickers/labels

Some companies claim they generate or print certain shape or graphs on the label whose photo can be taken and sent to the cloud servers to authenticate.

Unfortunately, they are still the same, no matter what the company claims about running a Machine Learning or AI to scan the image on the cloud. The truth is anyone who can take photos of the sticker and print them on a paper would pass the counterfeit-check.

As long as the server gets the same scanned photo, regardless of the source (genuine sticker or copied sticker), it will pass the check.

RFID Tags/Labels

RFID is no different than holograms when it comes to copying them. It is even easier, a you need is the RFID code set in one of the original item and set the same code in cloned RFID labels/tags, and you will be ready to pass the counterfeit check!

Usual cost varies from few cents to dollars based on type of RFID tags (active/passive).

Unique Random Code per Product (QR or Barcode or number or text)

Companies, who provide the unique code per product, make more sense. There are tw type of Codes usually provided:

A. Open (visible to everyone even before purchasing the product

If the codes are open (not protected by some scratchable layer), then it is of not much use, anyone can copy them and pass the counterfeit check, no matter what company claim about the crypto tech or AI tech they use in the backend (although with the help o geo-location tech and AI, red flags can be raised for some cases).

Truth is, if you have the same code as the original, which you can see without buying the product, then you can copy it and pass the counterfeit-check.

B. Hidden or protected code

These are the physically protected QR or Barcode or Alphanumeric codes and you mus buy the item before you can see the code, for example, scratchable card, and then verify with the backend server.

This does protect the item and if the backend technology is implemented properly, i.e. non-guessable codes are generated, then this will prevent the counterfeit.

But problem is, user has no idea before buying the item if it will be genuine or not, not only this company who has not implemented the backend properly may pass some items which may be fake, or may pass already scratched code again and again.

Secondly, if their DB is hacked then it will be very simple for the hackers to sell the codes to Counterfeiters.

The development and more importantly maintenance and security of such system is not simple and usually costs good maintenance cost. And the authenticating servers will have to be always online.

Introduction of Neurotags Technology

Finally to provide better anti-counterfeit protection, we designed and implemented Neurotags technology. We kept mainly 3 things in mind:

1. Foolproof but semi open (user can check authenticity with decent probability before buying too)
2. Secure
3. Simple to use and efficient

Foolproof and semi open

This is the most difficult part to design. After careful thoughts, we have introduced two tags which go together, one hidden and one open and each is unique for each product.

User can scan the open tag before buying and get a good estimation of genuineness of the product and check any RED flags. And scanning the protected tag after purchase provides complete genuineness information.

There are two protection we have given to Open Tag:

- This tag is tightly mathematically coupled to the protected tag. So if someone buys the product and scratches and scans the protected tag, the open tag's status is also updated in our system. And any further scans of the open tag fails the counterfeit-check.
- If counterfeiter copies the open tag and replicates it, the first scan of the protected tag will invalidate all the products with corresponding open tag.
- Machine learning based anomaly detection system is always monitoring the scan activity of the tags. If the open tag starts to randomly appear from the geographic locations where it should not be or if the patterns of scanning has any anomaly pattern our algorithms raise the RED flags. Which would mean all the products of the copied tag would be invalidated, a counterfeiter has to put new copied tags on products in retail stores, which would again be caught by our system within few scans.

Protection to Protected Tag:

- Physical protection is provided to each tag, i.e they can only be scratched or opened once after purchase. Once they are scanned their status gets updated on our system and they can not be used again for authenticity check by any other device.
- They are mathematically coupled with the open tags. So any anomaly pattern on the open tags will lead to RED flagging of the closed tags too.
- Machine learning based anomaly detection system keeps monitoring the scan activity of the closed tags and the open tags. And immediately raises the RED flags for any abnormal or anomalous pattern.

Security

Security of the auth system and tags are the most important criteria in designing the system.
Being ethical hackers and experience fighting hackers in gaming companies in past (Gala Net) and designing the secure systems for finance companies (Paypal) has helped not to overlook any potential cases where security can be a problem.

We can not expose more here, but our tags info is one way "scrypt" and private key secured so even if someone gets the DB of tags he or she can not get the tags code.
Simple to use and efficient

We have provided iOS and Android app (soon Windows app is coming) to scan the Neurotags and manage the purchases, warranty of the products and access to customer support.

Codes can also be scanned by any scanner app specially popular apps, such as, WeChat in China.
The technology is cost effective, on the cloud and efficient to use so that it can be used by any company of any scale, without worrying about the cost.

Overall Value

The money saved by preventing counterfeits will always be many times more than the cost to use Neurotags.
The valuable insight of consumer behavior data collected with Neurotags will help improve the Business Intelligence.

Warranty and support modules can help up-sell the extended warranty protection and consumable parts of the products.

Bundling the loyalty programs with Neurotags would further increase the repeat sales.