Politecnico di Torino

Politecnico di Torino

INGEGNERIA GESTIONALE (ENGINEERING AND MANAGEMENT)
A.a. 2022/2023
Sessione di Laurea Dicembre 2023

Anti-counterfeiting devices for the automotive sector

Analysis of these solutions and benchmarking of competitors

Relatori:
Prof. Marco Cantamessa
Paola Dogliotti
Massimo Marensi

Candidati:
Giacomo Murazio

Politecnico di Torino

Politecnico di Torino

1. Introduction

The thesis subject refers to Anti-Counterfeiting solutions with an application with the automotive industry. The objective of this work was to explore possible solutions that FPT Industrial will be able to further analyze and use to protect their products from being counterfeited.

I have explored the possible solutions already present on the market and then I have focused on the one more interesting for the automotive sectors. I have collaborated with some colleagues during my internship in the company. The work is structured in three chapters where there is an introduction to all the solutions adopted to fight counterfeited goods, an analysis of the market in which counterfeit goods have been sold, and the final chapter which describes an Excel paper that I "created" with the help and assistance of some colleagues. The material was founded through research on Internet, report that the company already has in its possession, and through competitors' website and newsletters.

1.2 Technologies used for anti-counterfeiting

The vast realm of anti-counterfeiting technologies presents a myriad of diverse solutions, each meticulously crafted to uphold ownership rights and preserve the integrity of legitimate supply chains. Amid the ever-evolving landscape of technology, this domain often proves to be intricate and elusive, as the array of available technologies continues to expand, shrouding comprehensive information in a veil of complexity. In broad terms, anti-counterfeiting technologies offer an intricate toolkit tailored to a critical mission: the validation of a product's authenticity and the detection of any ominous traces of forgery or fraudulent activities that may have tainted its journey. These technologies employ a wide spectrum of methodologies, spanning from the attachment of remote sensors to products to the covert embedding of markers concealed within their very essence. Nonetheless, their unwavering dedication lies in the execution of one or more fundamental functions:

1. Authentication: At its core, this function rigorously verifies the purported identity and attributes of a product.
2. Tracking/Tracing: An indispensable process that unravels the intended locations and the past or present whereabouts of a unique item navigating the intricate web of the supply chain.
3. Anti-tampering/Anti-alteration: This facet encompasses a range of mechanisms and techniques ingeniously designed to fend off any endeavours to tamper with a product, ensuring that alterations, falsifications, or unwarranted interventions are kept at bay.

Given the multifaceted requirements of various companies, the spectrum of available anti-counterfeiting techniques unfurls in a remarkable tapestry of diversity. The choice of technique hinges on the distinctive blend of essential functions they offer, the methodologies they employ, and the mode through which verification is executed. This spectrum ranges from approaches discernible through human senses to those necessitating the involvement of specialized devices for validation. Frequently, these technologies intertwine

and collaborate to meet the intricate demands, culminating in an elevated level of security. Factors such as reliability and cost play a pivotal role in guiding the selection of one method over another.

A unifying thread that runs through all anti-counterfeiting methodologies is the integration of distinct marking devices, aptly christened as "markers." These markers are seamlessly integrated with the products, employing an array of techniques to ensure their inseparability, and housing the indispensable information that empowers the technology to efficiently fulfil its designated function.

1.2.1 Electronic Technologies

Every electronic approach to combating counterfeiting hinges on the convergence of electronic data devices and products, establishing a unique bond that serves as the linchpin of their identification, authentication, and meticulous tracking. In this realm, the end products acquire a distinct identity and are endowed with the capability to engage with a comprehensive web of electronic technologies. These electronic devices, which we will delve into in the ensuing section, function as reservoirs of invaluable information. They may either directly transmit specific product-related data or facilitate access to a reservoir of comprehensive data stored in a dedicated database. Embarking on an investigation into the realm of electronic anti-counterfeiting technology reveals a varied terrain showcasing five distinct archetypes, each endowed with unique capabilities. Yet, it is the widespread acknowledgment earned by Radio Frequency Identification (RFID) and Near Field Communication (NFC) devices that truly captures attention. These technologies are veritable maestros of remote object, animal, or human recognition, elevating the battle against counterfeiting to new heights. The five archetypes are as follows:

1. RFID (Radio Frequency Identification): A technological juggernaut renowned for its prowess in the wireless identification of objects.
2. NFC (Near Field Communication): An emblem of close-range communication capabilities, enabling seamless remote recognition of objects, animals, or individuals.
3. Electronic Seals: These robust devices serve as the gatekeepers of authenticity, preserving the sanctity of products against unwarranted intrusion or tampering.
4. Magnetic Stripes: A stalwart technology that leverages magnetism to safeguard data and fend off counterfeit endeavours.
5. Contact Chips: These intricately designed chips stand as sentinels of product integrity, serving as a bastion against fraudulent activities.

Each of these electronic anti-counterfeiting technologies, with its unique attributes and specialized functionalities, plays a pivotal role in safeguarding the authenticity of products in a dynamic and ever-evolving landscape.

1.2.1.1 RFID

RFID uses radio frequency technologies to recognize objects, animals, or people remotely. This method is executed by two devices that work tighter to protect the final good and to transmit information. The first

device is called “Tag” and respond and transmit through radio frequency channels to the second device, portable or fixed, called “Readers”. The reader has also the function to pick up the information and any other data contained in the tag. If a reader is connected to the internet, it will be possible to monitor data in real time. The security provided by these solutions depends on the communications protocol that will be selected, used between tag and reader, and the protection layer used to store and protect the information inside the tag.

Considering these factors, RFID technology finds practical application in Internet of Things (IoT) solutions and is extensively employed in anti-counterfeiting measures. An illustrative instance can be observed in the domain of 'smart labels,' where RFID tags are seamlessly incorporated into adhesive labels, infusing them with intelligent functionalities. While various iterations of RFID technology exist, they all revolve around a fundamental trio of components:

- Tags: Attached to goods, these consist of an antenna and a microchip housing product data.
- Readers: Responsible for interrogating the tags, transmitting or receiving information, and conveying it to the data processing system. The specificity of RFID readers aligns with the chosen RFID tag type.
- Data Processing System: Connected to the readers through the internet, this system utilizes identification codes from the tags to access and manage all pertinent information related to the objects.

Prominent RFID types encompass Passive RFID, Active RFID, BAP, and PUF.

2.2.3.2.1 Passive RFID

Passive RFID tags are composed by an antenna and a microchip, an integrated circuit. The reason why these devices are called passive is that they have not an internal power source, but they are activated by a RFID reader which transmits electromagnetic signals. Upon activation by the reader, the tag transmits its enclosed information to the reader, which subsequently communicates the data to a computer for processing and verification. There are two kinds of passive reader, read-only and read-write which allow the user to modify and/or rewrite the data stored inside. Due to its nature these devices have limited power, low read range that based on the frequency used could be identified as low frequency (few centimeters) or high/ultra-high frequency (few meters).

Passive RFID have a large number of applications, they can be easily incorporated into various goods which range from small objects to adhesive labels or directly into products. Some common uses are credit cards, buttons, bottle caps, keys, sheets of paper, banknotes, and entry tickets. Validating the genuineness of the product involves the retrieval and interpretation of data stored within the RFID tags. The verification of the information stored or the check of the tag (to see if someone has tried to tamper it) is done by specialist staff at retail outlets, with the appropriate equipment. The needs for staff to verify it will avoid the possibility to independently authenticate products by consumers.

Since passive RFID could be of different forms, sizes, uses and other characteristics, the implementation requirements required by a company to use it are highly specific. In the case you want to affix them directly into your products then specific changes will occur to the production chain. If, however, you will use a label or a similar device (bought or produced) you will have to just choose the most suitable from the range available and affix it to the desired product.

The tags that are present on the market are generally small with a cost starting from few euro cents per tag.

Figure 1

2.2.3.2.2 Active RFID

Active RFID devices are very similar to Passive RFID, both have a tag and a reader, but the active tag is composed by its own power battery, a transmitter, and a receiver alongside the antenna and the microchip. The battery inside the tag provides them with unique feature that improve how they function. The battery enables larges memories, which are often rewritable, and usually use high frequency (sometimes also called ultra-high or super-high frequency) which allow these tags to support greater distances than passive and semi-passive tags, depending on some technical factors the range could be around 200 meters.

Active RFID tags are suitable to be used with high value goods, due to the more features that they possess. They also have additional functions such as radiolocation (RTLS-Real Time Location Systems) and the measurement of environmental parameters through sensors (temperature, movement) also make them attractive to logistic operators, for example to track cold food. These functions make them perfect for product tracking both within companies and between them.

These tags are bigger in size than passive ones, due to battery and the shell that is needed to protect the technology inside. Moreover, these tags can be reused and operate on high frequencies (UHF, SHF) making them perfect to protect more valued goods. The bigger size and the presence on new technology equipment, such as a battery, make them more expensive than the passive tags. Active RFID have a cost that could be tens or hundreds of euros per tag.


Figure 2

2.2.3.2.3 BAC

BAC tags have a battery which power only the integrated circuit, like Active tags, in this case they have a smaller battery that could be run and store information through the utilization of sensors which could be environmental among other possible types of sensors. This kind of tags could be known as semi-passive tags because although they possess a battery, they do not include a transmitter inside the tag (main difference from active ones). They function as a passive tag; they are activated by a reader. This small battery enables a range of use between passive and active, usually they can work around 12 meters but never more than 30 meters. One of the main disadvantages is the life of the battery and its disposal at the end of is useful life, but these problems could be exceeded by new technology such as solar energy or inertial systems to power the battery, like solar-powered wristwatches.

The main application for this kind of tags is the “cold chain” which is the control of temperature, usually to keep frozen, during production and distribution of some goods such as food.

The cost of these devices depends on the battery and its alimentation/powering systems and usually is around few euros per tag.


Figure 3

2.2.3.2.4 PUF

As we have seen every tag contain a chip, every chip could be unique due to random and uncontrollable microscopic imperfections in the molecular structure of it. PUF tags exploits these imperfections to create

unique chip that will use its uniqueness to prove authenticity. Then the unique chip could be stored in different databases that will be used to check and verify the microscopic imperfections present in a chip.

There are several material or technology to produce PUF chips, but the most used in RFID tags is silicon based PUF technology. This material generates random unique identification codes based on their intrinsic physical variations. PUF methods are a new way to create unique chip called “on-chip” keys, that are cryptographic keys for secure information exchange.

Since PUF technology is applied on the chip, it could be used in the same applications and with the same functioning as the RFID tags (passive, active, BAC). Usually, the cost of this technology reflects the cost of the RFID tags in which is it applied on.

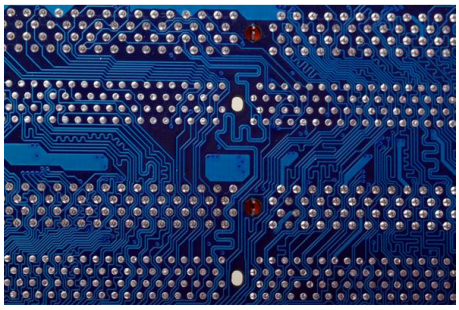


Figure 4

1.2.1.2 NFC

NFC technology is used to enable wireless payment between a device and an NFC-enabled payment machines, it is already widespread in smartphones such as Apple Wallet where we register a card on the phone.

NFC technologies have been developed from contactless card and RFID technologies; it has some similarities with RFID tags. It moves away from the rigid distinction between tag and reader, NFC systems could be both a reader and a tag, and from passive and active definitions since it could work in both active and passive mode. NFC technologies could be summarized as a set of communication protocols for secure wireless communication that could operate in distances less than 10 centimeters. It also operates at different frequencies, 13.56 MHz. The main disadvantage is that it could only communicate with one devis per time, while some RFID systems are able to communicate with multiple devices at the same time. NFC tags can be placed on credit card, paper label or smartphones. Since almost all smartphones hold an NFC reader, consumers are able to check the authenticity of products with their own devices, a thing that with RFID tags is not possible.

The cost of these devices is very similar to passive RFID tags, is slightly more due to the more functions that they provide, and it is around few dozen euro cents per tags.

Figure 5

1.2.1.3 Electronic Seals

Electronic seals are used as mechanical seals, but they enable the possibility of recording important products information such as real time tracking and monitoring, sometimes that could also self-monitor themself. When a seal Is broken is a clear indication that the object has potentially been tampered with. Another feature is that usually when tampered with, they trigger an alarm. Electronic seals, also called eSeals, have been developed from RFID technologies to store digital data and readability functions. The two main objectives of an electronic seals are to guarantee:

- Integrity, by clearly showing that the seals has been broken.
- Identity, by uniquely identified the product (like a container) to which is applied.

Moreover, an electronic seal could have also mechanical properties that combined with “digital” ones offers even a more unbreakable seal. The quality characteristics of these kind of seals are: non-duplicability showing that it will not be easy to replicate it; reliability by showing that has been clearly opened or that once opened could not be resealed; verifiability by an operator that should be able to check its authenticity and integrity either visually or by using a specific device.

eSeals are mostly used for logistic application, in the supply chain during the distribution and transportation process like on container through sea routes. These devices are chosen for this utilisation since it offers mechanical properties and it can store different information inside of it such as route information, the container ID and the details of the cargo being carried and real time data. Then the seal could be checked through visual inspection, by looking at the aspects and mechanical properties, or through specific devices to read the information stored.

The cost depends on the type of RFID tag (active, passive, BAC) used and the mechanical properties. These devices are applied on end-products and so no changes are needed in the production process. They have a high cost due to the high level of protection that they provide, also considering the real-time information.


Figure 6

1.2.1.4 Magnetic Stripes

Magnetic stripes are the black line present in almost every credit and debit card. It usually found on the back of the card that could be a payment card or an identification card. The data contained in this stripe is scanned when it is passed/swiped through a card reader.

Due to its nature this kind of protection devices are mainly placed on card following international defined standards that the card must comply to support this technology. These standards are used to regulate size, flexibility, position of the magnetic stripe, magnetic characteristics, and data formats.


Figure 7

1.2.1.5 Contact Chips

Contact Chips are specific microchip embedded in plastic card. The microchip contains unique information that could be read only by inserting the chip into a card reader. The most used card contains this chip are pre-paid card or hotel rooms keys. Contact Chips cards are usually categorized based on their microchips' characteristics:

- Memory card
- Microprocessor card

Figure 8


Figure 9

1.2.2 Marking Technologies

Marking technoligies, as their name suggest, work by applicate a mark/stamp on a product. This mark carries unique security features such as graphic patterns or codes. Light radiation, visible or invisible, is used to recognize graphic pattern (holograms). Graphic patterns are used for simple authentication, while codes that usually are barcodes are used also to provide a unique identification. The security level that they provide is established by the nature of the technologies itself, the chemical and physical characteristics of an ink, or the information it contains, in a graphic pattern. There are several different types of marking technologies:

- Optical Memory Stripes
- Machine-Readable Codes
- Security Holograms
- Inks
- Watermarks
- Microtexts
- Gulloche/Rainbow Painting
- Unique Identifier Marks
- Copy Dtection Patterns

Verification can be performed easily by a visual inspection or through a smartphone. The most used are the ones which could be inspected visually, has a low cost per item and require very easy verification procedures.

1.2.2.1 Optical Memory Stripe

An optical memory stripe is a laser device used to read magnetic stripe. It can store data and also images and it has a relatively high memory (up to 4 MB). This device only read information, it is called read-only device, so it will not be possible to modify or update the data stored through the product “lifetime”. The optical memory stripe could be attached to the good it is identifying a tracking or to be affixed on a card such as an electronic identity card.

Figure 10

1.2.2.2 Machine-Readable Codes

Machine-readable codes are codes that could be read through several devices, usually an optical scanning device. Typically, this identifier is known as barcodes, consisting of a sequence of parallel black lines and white spaces or dots and squares (even incorporating a combination of both for enhanced security) with varying widths. In the codes are stored the various information needed about the product like place of manufacture, owner, origin, expire date, product code, etc. the most used machine to read these codes are laser beam and through the camera of a smartphone which also enable consumer inspection. There are two types of codes currently used:

- One-dimensional code (linear, figure 11)
- Two-dimensional code (matrix, figure12)

One-dimensional code, also called barcodes, are represented as a single row of bars in which data are stored horizontally. The size and shape of the lines determines the quantity of the information stored as the level of security and readability which will be maintained in case of adverse physical conditions, or the label is damaged. The width of each line determines the quantity of information stored in it, it is possible to extend/reduce the information stored by increasing/decreasing the width which quickly reaches a limit beyond which reading the codes will become impossible or very difficult. To simplify and to enable humans to read this code, barcodes are usually accompanied with a plain text. There are standards which regulate the accepted character (numerical, alphanumerical, special character) and the maximum number of characters or digits. For example, Code 128 can encode up to 128 different symbols or Code 39 that can contain 39 symbols, then there are codes with a fixed length such as EAN 13 has a fixed length of 13 digits, while UPC has a fixed length of 12 digits.

These kinds of codes can be easily found in the form of label or can be easily attached directly onto the products or packaging.

Cost depends on the cost of printing them or on the cost of a label on the market.

Two-dimensional codes are also known as matrix barcodes or matrix codes. The matrix uses a series of dots, spaces, and squares to store information both horizontally and vertically. These codes show a larger capacity due to the possibility of storing information also vertically. One dimensional code is used together with a

relevant database, instead this matrix can contain all the information required to identify a product inside of them. Two-dimensional code provides, in case is required, a unique URL which is used to access to a cloud to retrieve important or additional information. Even if there are several two-dimensional codes, the most used (even for different application and sectors) is the QR Code and the 2D Datamatrix.

QR Codes themselves do not offer great protection against copies, but when combined with different technologies such as holograms, copy detection patterns, and unique identifiers, they became very effective. Due to high memory possibility QR Codes are becoming more popular.

Costs are determined by the cost of printing and the price associated with any supporting/backing labels used. An important factor that could influence cost is the implementation of a content/client management platform for those codes that contains an URL link. The platform will serve as a tool for overseeing the codes, the associated data for each code, and delineating specific interaction levels tailored to each user category.

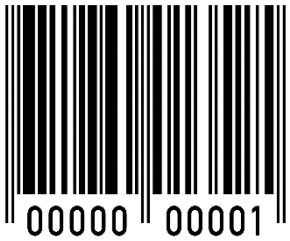


Figure 11


Figure 12

1.2.2.3 Security Holograms

Holograms are devices that work based on visual effects that change based on angle, lighting, and perspective of who is looking. This technology is based on diffractive images called DOVIDs (Diffractive Optical Variable Image Device). The variation of the viewing angle is the mechanism which create three-dimensional images. To create a hologram are used machines, photographic, which record the light scattered from an object a then present it in a way that look like a three-dimensional image (holography). The main advantage of this technology is that hologram cannot be duplicated by colour printers, scanners, and cameras because these machines reproduced images at the same angle, it is not possible for a scanner to scan different angle. Holograms are used to authenticate products, not to identify them, through the inspection and comparison of the hologram on the product with the original stored in a database. There are various type of traditional holograms and different methods for making them:

- Multi-layer 2D-3D holograms: The 3D effect results from the layered depth of multiple levels of 2D holograms, distinct from an optical illusion.
- Singular 3D holograms: In these holograms, the image encompasses three dimensions length, breadth, and depth. The three-dimensional effect stems from a physical model emerging from the holographic plane, where the holographic image encapsulates the entire information set of the wave front emitted by an illuminating object.

- Dot-Matrix: several tiny dots, with a separate diffraction rating, are used to create a 2D or 3D image. The dots, that measure several tens of microns in size, are too small to be seen by the human naked eye. This is one of the most used methods in the anti-counterfeiting technologies.
- Hot Stamping Foil (HSF): this method consists in the dry printing of lithography at high temperature, pre-dired inks or foils are transferred to a surface through high temperature. It is widely used on paper and plastic products, but due to its nature could be applied to different materials if they will tolerate high temperature.
- Holograms obtained by de-metallization process: the hologram is obtained by applying aluminium onto the holograms itself and then by removing it in a graphic pattern. To provide stronger security it is possible to make printouts that metallized and transparent parts on the same film.

Traditional holograms could be applied to almost all materials and products. The cost depends on the methods and the kind of holograms selected. It will be relevant also the technique used to attach it to the final goods.

Complex holograms (figure 14) are very similar, they have the same appearance, to traditional holograms (figure 13). Complex holograms have two layers of protections since they provide visible and invisible information. The visible layer enables easy and fast authentication through visual inspection. Within that image there are some information that are hidden through the use of hidden/micro text, encoded information (cryptograms) which could be only read through the use of special devices such as special lenses, microscopes, lasers, and CD players.

It is not possible to identify or establish the cost of complex holograms without knowing the products on which it will be applied, and the nature and methods used to store visible and invisible information.

Figure 13

Figure 14

1.2.2.4 Inks

Ink-based technologies are used to mark products with different inks that will be used to authenticate, and in some cases to identify or track products which contains a unique product identification code in the marking. There are several inks used nowadays, they are cheap, relatively easy to apply, visible, and invisible. This ink is used mostly to mark paper products such as paper valuables, banknotes, and documents. Invisible inks are used to:

- Avoid altering the appearance of the product.
- Avoid interference with subsequent product.

- Prevent easy detection by potential counterfeiters.

They may be distinguished by the different way to read them, or the reading tools used, their reaction to chemical procedures.

2.2.3.2.1 UV-Sensitive

UV-sensitive ink is a special ink that reacts accordingly to the ultraviolet light (UV light) at which it is exposed. Its fluorescent pigments show a shade when exposed to daylight and another one when exposed to UV light. The only method to detect and verify this ink is through the use of a “Wood’s lamp” that is a light source that emits electromagnetic radiation in the ultraviolet range, but it is also visible in the light range. This technique is used consistently since the 1960s to manufacture and protect paper. There are some special inks which offer even a heightened protection and difficult to reproduce, such as photochromatic and “ghostly white” because are very difficult to find.

The cost varies accordingly to the types of inks used, as mentioned before a photochromatic ink will be more secure but will also cost more than a “normal” UV-sensitive ink.

Figure 15

2.2.3.2.2 IR-Sensitive

IR-sensitive inks are similar to the UV-sensitive, but instead of us UV light they used the infrared range. This ink is completely invisible to the naked eye and could be only read by special devices, called infrared readers. This ink could also appear as transparent or opaque. This technology works by using the “meta-material” inks which are pairs of various colors that appear as one in the daylight but when exposed to the IR light become mismatched. They are also used to hide barcodes.

As for the UV sensitive, it is difficult to have a general idea of the cost of one ink, because it depends on the product chosen. IR inks are mostly used on paper and the have a longer life than UV ones.

Figure 16

2.2.3.2.3 Magnetic

This category of inks exploits the magnetic properties of some object or materials, in particular these inks have pigments which react with magnets. The inks, also called “magnetic flakes”, can be detected and read only by special devices. Magnetic inks are usually used for the serialization and numbering on currency; however, they could also be used to encode information on a document. The magnetic barcode that will be generated will give the possibility to read information, and to authenticate the document. MICR (Magnetic Ink Character Recognition) is the most used ink methods to number cheques in different countries, the set of character running along the bottom which is specified by the ISO 1004 standard.

2.2.3.2.4 OVI and Irisdescent

Optical variable inks (OVI) and irisdescent inks exploit different viewing angles to represent different colors. The pigments show a color based on the angle of the viewer, usually the colors are in pairs such as red-green, gold-silver, and green-blue. This ink is very difficult to reproduce because normal copiers and scanners cannot replicate the color change effect. In fact, these machines can copy a document at a fixed angle relatively to the document’s surface and so reproducing only one color. OVI inks are one of the best anticounterfeiting technologies, the fact that is almost impossible to reproduce or that will be need expensive copiers grant a higher level of security.

Irisdescent inks are very similar to those just illustrated, based on pearled, pearlescent, or mother-of-pearl colors that contains pigments made of micra particles which when viewed from different angles display a different intensity of colors.


Figure 17

2.2.3.2.5 Thermochromic

Thermochromic inks, instead of using the light variations, use the temperature changes. Even a small variation such as finger rubbing can trigger this ink. The color change could be reversible, the color will return to the original once the temperature will return at its original value, or irreversible. Beyond this classification, thermochromic inks are divide into the ones that are triggered by heat or by cold. When ink becomes transparent, the underlying background becomes distinctly visible. The transparency of ink is influenced by factors such as temperature, colour, dye concentration, and thickness. Notably, the temperatures at which inks typically lose around 95% of their colour are standardized at 6°C and 31°C.

These inks could be applied on a vast range of products of packaging. It's essential to note that, while they provide excellent reliability, their colour sensitivity can degrade or vanish when subjected to prolonged exposure to elevated temperatures (beyond 50°C), UV light, specific fluorescent lighting, and excessive sunlight exposure.

2.2.3.2.6 Reactive

Reactive inks, as the name suggest, work by reacting to different aqueous solutions, solvents, and other chemical agents when they are encountered. There are several forms of reactions such as erasure, discoloration, color transformation, running, staining, and smudging. All these forms indicates that the good have been tampered or altered. These inks provide an immediate and visible indication of any attempt of tampering.

Consider, for instance, a document with inks designed to vanish or alter colours when tampered with. This makes it easy to detect any such attempts due to the observable reaction. Reactive inks come in three primary types:

1. Erasable inks: Comprising water-soluble dyes and resins, these inks are suitable for typography or dry offset printing. Some countries utilize erasable inks to safeguard their checks, typically as a background feature.
2. Solvent-sensitive inks: Reacting to common chemical agents employed in anti-counterfeiting measures, such as bleach, alcohol, or acetone. Exposure to these agents prompts the ink to run, change color, or induce a stain, thereby exposing any forgery.
3. Fugitive inks: Like the previously described inks, these substances react to water or an aqueous solution. The ink runs, causing the printed areas to appear smudged, thereby revealing any forgery.

The cost of such inks cannot be predetermined in advance.

2.2.3.2.7 Penetrating

Penetrating inks, also known as “bleeding inks”, work by permeate through the paper substrate. These inks are applied by penetrating deep into the fibers of a paper documents creating a week stain around the print that is visible on the back of the document. When someone is trying to alter, mechanically erase, or scrape a number the ink will react causing visible damage and leaving a stain on the document. An alternative method

for applying this ink involves blending it with a coloured oil capable of deeply infiltrating the paper's pores, resulting in the formation of a coloured stain around the designated number.

To apply this technique, you will need to adapt your printing process to be sure to support this ink the to place it in the desired position on the paper.

The cost associated with this type of ink will depends on the technique used, the paper in which the ink will be placed, and the deep that has to be reached by the printer. It is therefore difficult to establish the cost before the process has been chosen.

1.2.2.5 Encrypted Images

Encrypted images or information are code hidden into photographs or into the background of documents. This technology grants a higher level of security due to the fact that encrypted information is not visible to the human eye. They can be viewed by using special decoding lens (special viewer) or with laboratory equipment, usually a scanner or a video camera connected to a computer equipped with a specific image processing software. The encrypted information is applied in an encoded format; thus, another layer of protection will be present in the case the counterfeiter will use special lens.

Encrypted information is mostly used on paper, documents, and travel documents. In passports, for instance, the country's name can be seamlessly integrated into the background of the pages, or the holder's personal information can be discreetly concealed within their photograph.

Figure 18

1.2.2.6 Watermarks

Watermarks stand as one of the earliest technologies devised to safeguard paper, such as banknotes, from the perils of counterfeiting. These are designs, images, or patterns seamlessly integrated into the paper during the manufacturing process. Their production is straightforward, involving the application of pressure to the substrate in the form of a pattern or text, causing the paper to compress only in the specific areas where pressure is exerted. One technique involves the application of dry watermarks by guiding a device known as a dandy roll over a slightly moistened sheet of paper. The roll may be covered in thick paperboard, upon which the intended wording or figure is designed in relief using wires, gels, or other implements. Watermarks are visible to direct light, like a banknote that has to be raise by the table and placed under a lamp to reveal its watermarks.

These methods are mostly applied to paper documents, will be very difficult to implement them on other materials.

Figure 19

1.2.2.7 Microtexts

Microtexts, as the name suggest, are very little (micro) texts inserted into a document. With this technique it can be possible to miniaturize a text or even an entire document that in the most cases will be read by special machines/equipment. The advantage of microtexts is that for the human eye, copiers, and scanners it will be seen as a solid line. Because of its size, microtexts are printer or applied by specialized machine such as laser-engraved matrices that use special inks and techniques which will guarantee to reproduce with extreme precision the graphical details.

Figure 20

1.2.2.8 Gulloche/Rainbow Printing

The Gulloche technique takes its name from the French term "guilloche," denoting an ornamental design crafted from engraved metal plates. These patterns are created by special software and mechanically printed by specialized machines. The design is crafted with repeating linear or undulating lines, incorporating seamlessly blending colours and intricate relief effects that pose challenges in reproduction. It is possible also to predetermine a color shift, creating the illusion of synchronous animation.

Rainbow printing is a similar technology that could be sometimes implementer or combined with the gulloche. As for other techniques that have been seen previously, it will not be possible to reproduce it

through normal copiers or scanners. It is a technique which subtly merges the colors into each other resulting in a gradual color change that remind a rainbow.

 Figure 21

1.2.2.9 Unique Identifier Marks

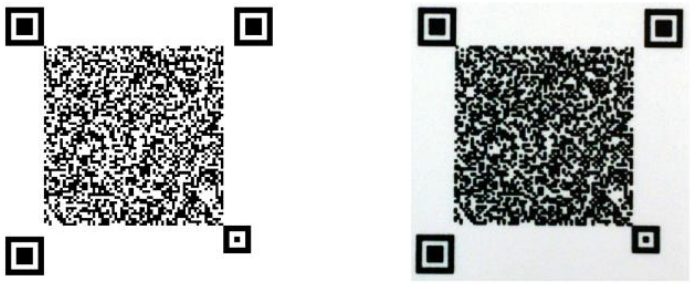
With this method are inserted into a document visible or hidden identifiers that are unique. They are generated by random and non-replicable chemical and physical process, and when are visible, they appear as an unintended inks spots or smudges. A particular printing technology can be used to create small and colored patches that will be unique, original, and will be asserted as a unique identifier such as a fingerprint works for humans. Then a numerical code, called its signature, is assigned to each unique identifier to store them in a database. There is not an optimal method to create them, and so there are different methods that will generate unique identifier.

1.2.2.10 Copy Detection Patterns

Copy detection patterns, also known as secure graphics, have been studied to avoid counterfeiting by eliminating some information stored inside when scanned, regardless of the quality of the scan. They are small, random, or pseudo-random digital images. CDPs, copy detection patterns, are maximized to reduce the loss of information when scanned. Authentication is done by an algorithm that will check the information contained in the two images, because of its principle the image on the final good will be scanned at least one more time than the original, thus containing less information. The authentication could be done by special devices or readers, scanners, or through phone camera and then checked via a mobile phone app. Copy detection pattern could be also inserted into other technologies, such as 2D barcodes (QR Codes or data matrix), for enhanced security which will also facilitates smartphones authentication and improves traceability.

Since the integration of the process is essentially digital there will not need to make any major changes to the production or logistics operations.

The cost associated to this technology will depends on the technique and the database used to produce and store those code.



(a) Binary digital template. (b) Printed original code. Figure 22

1.2.3 Chemical & Physical Technologies

Chemical and physical technologies are based on special substances which create unique/random pattern when certain chemical or physical process are applied to materials. These patterns will serve as markers and will be used to identify and authenticate the products. The particularity of these technologies is that these markers are used for authentication instead of being used for product identification. This marks also result as very complex to replicate, since every reaction contains random pattern and properties.

While the expense for applying and creating markers is comparatively low, the specialized reading devices can be prohibitively costly. Consequently, it's essential to consider that instant on-site verification might not always be feasible, leading to the necessity of conducting tests in laboratories, which entails additional time and expenses.

1.2.3.1 DNA Coding

DNA coding is based on the principle of the human DNA which contain a unique sequence of genetic information, also called genetic fingerprint, that could be used in forensic investigation, in determining paternity, and detecting genetic health conditions as examples. The same idea has been implemented to combat counterfeiting, a unique DNA code is implanted into a product or package, rendering it traceable, identifiable, and verifiable. This technology results to be compatible with all kinds of materials proving to be applied on alcohol bottles and their labels, perfumes, refined fuels, and banknotes. It has been used with success in the mechanical, food, pharmaceutical, textile, and petrochemical industries with a widespread application in the packaging companies. The approach employed to incorporate DNA coding involves the insertion of molecules containing uniquely generated codes. These codes can be altered, resulting in an almost boundless array of distinct markers. These markers serve the purpose of identifying each of the safeguarded articles. The advantages ae that these tags are not visible for the human eye and are stable and permanent. The material ratio is miniscule, it is really fast top apply and only the smallest amount is needed, which leaves the product properties unchanged. These technologies are non-toxic and have a low environmental impact.

Legally acknowledged as a security system, this technology holds admissibility in court proceedings for substantiating wrongdoing under national laws. Nevertheless, owing to its inherent nature, the presentation of specific forensic tests may be necessary to bolster the furnished information.

It is not possible to estimate the cost of these solutions since the technology available on the market is controlled by the patent holders.

1.2.3.2 Chemical Encoding and Tracers

Minuscules particles, with specific chemical or physical properties, are used to authenticate and secure products and packaging. The size of this particles makes them invisible to the human eye and attachable to any surface. Special equipment is needed to detect the unique properties of these particles, these specialized machines are able to identify the particles that are present in nanometers (nm), that is a billionths of a meter, in length. They can also function as an origin marker or be applied to specific components to indicate product quality. For instance, in the case of a garment purported to be made of 40% cotton, a chemical tracer could be introduced to the cotton yarn during the initial stages of production. Many years later, even after the garment has been purchased and used, a dedicated reader can still measure the quantity of the chemical tracer present to verify the cotton content.

Furthermore, the particles embedded in the raw materials are encoded to enhance an even higher level of security. There are several chemical encoding and tracing methods used nowadays, such as chemical compounds with optical properties or compounds with physical properties like magnetically attractable particles.

Due to the high combination of methods, chemical and physical properties that could be used, it is impossible to give a general idea of the cost involved in the implementing of this technology.

1.2.3.3 Glue Coding

Glue Coding exploits a process applied with a polymer that will generate spontaneous, random, and unique bubbles to form in it. The process consists in apply heat to this polymer that will result in different position, size, and shape of bubbles every time making each combination as unique as a snowflake. Each bubble is a unique and not replicable 3D pattern very similar to a fingerprint. There are no constraints in term of size for the bubbles, even for the tiniest pieces of this polymer (a few millimeters) and then attached to the product where they serve as the item “signature” or seal of authenticity. These bubbles, that could be seen as a three-dimensional pattern, are essentially impossible to replicate, making them ideal for protection against counterfeiting.

Each combination or each bubble pattern will be stored into a database, accessible only to the product owner. Then when the bubble will need to be verified an authenticated, a special reading device will analyze both two-dimensionally and three-dimensionally and compare it to the database references. Among the methodologies generating unique identifiers, this technique stands out as one of the most secure, with the likelihood of producing two identical configurations being approximately one in several billion.

It is not possible to have information regarding the cost before having chosen the attachment method and the database capacity.

1.2.3.4 Surface Fingerprint and Laser Surface Analysis

The surface of a product can exhibit distinct microscopic variations induced by various chemical or physical processes or substances. Leveraging this distinctiveness, technology assigns a code to each surface, forming a random and stable pattern akin to a fingerprint. These methods exploit physical random processes, ensuring a unique identifier that cannot be replicated or forged. Specialized machinery is essential for scrutinizing and comparing the composition and structural discrepancies of surfaces with the original.

A technique utilizing surface fingerprint technologies and laser surface analysis is employed to create labels incorporating a nanoparticle coating with silicon polymers. The desiccation of the coating induces narrowing and generates structural variances or "wrinkles" on the polymer. Analysing these "wrinkles" facilitates the random generation of unique identification codes. These labels can be effortlessly read by an optical reader.

The cost will depend on the method used to create the surface differences and thus cannot be calculated in advance.

1.2.4 Mechanical Technologies

Mechanical technologies delve into the physical nature of materials to combat counterfeiting and establish robust anti-tampering defences. When operating in isolation, they undertake straightforward validation tasks, but their potential broadens when integrated with other technologies, enabling them to assume roles in identification and tracking. As an illustration, product labels can incorporate distinctive identification codes to enable seamless traceability. Most of the mechanical solutions manifest as a diverse array of labels, which can be categorized based on their physical attributes, encompassing the materials used and the methods of attachment to the product. Typically, labels call for authentication via automated reading apparatuses, such as barcode scanners. Nonetheless, for alternative mechanical approaches, such as laser engraving, authentication can be visually executed. The cost per unit for mechanical solutions typically falls within the medium to low range, and, particularly in the case of labels, their implementation is characterized by rapid deployment, often requiring only minimal alterations to the production process.

1.2.4.1 Labels

An identification label takes on the role of a tangible component containing essential identification data and product details, which finds its place either on a product or its packaging. The materials predominantly in use for crafting labels encompass paper and plastic film, generally featuring printed information on the front side and an adhesive layer on the rear, often referred to as adhesive labels. The materials utilized, adhesive type, support materials like silicon paper, the printing technology, resistance levels against environmental elements, and the intended purpose all exhibit variability.

These identification labels can be affixed to an extensive range of packaging and containers, including cardboard boxes, glass bottles, jars, plastic bags, and can even be directly applied to the products themselves, as seen in the case of clothing or footwear. When evaluating implementation possibilities, it's prudent to consider whether it might be more cost-effective to incorporate specific solutions within the artwork that will be directly imprinted onto cardboard, plastics, or shrink sleeves, thereby avoiding the need for adjustments to the standard production process. Labels also offer the potential for synergistic integration with diverse security technologies. When they are combined with technologies like radio-frequency identification (RFID) tags or near-field communication (NFC) devices, they transform into "smart labels."

2.2.3.2.1 Fabric Labels

These labels typically manifest as small pieces of fabric bearing essential information such as the brand name, company particulars, and product details like origin, size, content, and washing instructions. They serve as an effective means of product identification, particularly when combined with additional security measures like barcodes or holograms. Fabric labels can take two primary forms: woven or printed. In the former, the logo or text is intricately woven into the fabric, while in the latter, it is printed on the surface.

Fabric labels exhibit remarkable adaptability by allowing integration with various security features to yield labels with varying levels of sophistication. Simpler labels primarily display product information and identification codes, typically in the form of barcodes. More intricate labels incorporate advanced security elements such as holograms, security threads, and tracer fibres. The standard label sizes typically range from 20 mm to 70 mm, contingent on the product type and marketing requirements.

Woven labels, characterized by their fine thread, are most employed in the realm of clothing and accessories. This fine thread enables intricate detailing in words and patterns. Printed labels, on the other hand, find their place in clothing as well, often being attached or directly printed on the interior of the product.

Should you choose to adopt this technology, it becomes imperative to reconsider the method by which labels are affixed to your products. Robust stitching is a necessity, with the goal of making label removal result in visible damage to the product. Notably, the expenses tied to basic fabric labels tend to be quite economical.

Figure 23

2.2.3.2.2 Adhesive Labels

Adhesive labels, in essence, represent diminutive pieces of paper or other materials meticulously crafted to adhere to larger paper sheets or objects through a layer of adhesive on their reverse side. Analogous to fabric labels, adhesive labels fastened onto products feature printed identification codes, typically taking the form of barcodes, alongside essential product information.

The materials utilized for adhesive labels span a diverse spectrum, and their attachment methods vary accordingly. The adhesive component, in particular, is typically composed of rubber, acrylic, or an acrylic blend, contingent on the specific product and the environmental conditions to which the product will be subjected. Rubber adhesives exhibit commendable performance on a wide array of surfaces but show susceptibility to temperature and UV light compared to other adhesive types. Acrylic adhesives prove less suitable for plastic surfaces but offer heightened resistance to solvents and a longer lifespan. Meanwhile, acrylic blend adhesives, while boasting superior resistance, tend to wear off when exposed to heat and UV light.

Notably, the expenditure linked to uncomplicated adhesive labels tends to be exceedingly modest.

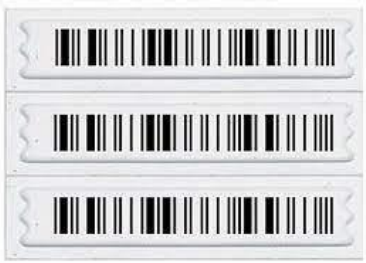


Figure 24

2.2.3.2.3 Labels with Micro-Engraved Cliché

Micro-engraved clichés are applied to labels using a hot printing process. These clichés are essentially metal matrices etched to replicate designs, images, photographs, and more. What sets micro-engraved clichés apart is the remarkably fine texture on their surface, featuring either random or repetitive designs that can be personalized to specific needs. When the hot printing process transfers this fine texture onto the label, it generates optical refractive effects. These effects cause the texture to change in form and colour when viewed from different angles, akin to the captivating appearance of a hologram.

The technique hinges on hot printing, a method that entails heating a die or matrix and pressing it onto a foil situated between the die and the object to be printed, which, in this case, is the label. Through this process, the intricate texture etched into the matrix is meticulously reproduced in both detail and colour on the label's surface. This not only enhances the label's visual appeal but also furnishes a reasonable level of protection against counterfeiting. This safeguard stems from the unique attributes of the cliché, rendering it a challenging task for counterfeiters to replicate.

The resultant effect bears resemblance to a hologram, albeit with a distinctive appearance and texture. Micro-engraved patterns can encompass an array of random or repeated designs and can be tailored with logos, bolstering their effectiveness as a deterrent against counterfeiting.

Importantly, the costs associated with implementing labels featuring micro-engraved clichés are generally modest and notably more economical than the expenses linked to incorporating holograms.

Figure 25

2.2.3.2.4 Sleeve Labels

The heat-shrink label, also known as a sleeve label, comprises a plastic heat-shrink tube made from materials such as PET, PVC, or OPS. Its unique property lies in its ability to conform to the shape of the product, enabling it to cover a portion or the entire surface. This versatile sleeve label not only guards against counterfeiting but also presents an aesthetically pleasing appearance to the end consumer.

In addition to its anti-counterfeiting function, this label can serve as a "certificate of origin" or a seal of authenticity on the container's cap. This added role ensures the integrity of the product by safeguarding it against potential tampering or alterations.

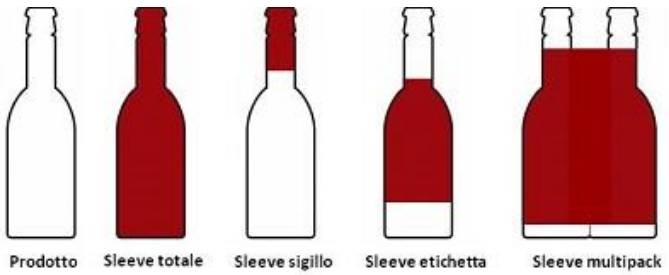


Figure 26

2.2.3.2.5 Ultra-Resistant Labels

Ultra-resilient labels are crafted from exceptionally robust, tear-resistant materials with the capacity to endure extreme temperature fluctuations. These labels are often coupled with concealed security features, such as invisible RFID tags or codes imperceptible to the naked eye. Their enduring strength and versatility make them well-suited for diverse settings, including both indoor and outdoor environments, as well as

hostile conditions. They find utility in industries related to shipping, transportation, outdoor storage, and industrial machinery.

The gamut of materials available for crafting ultra-resistant labels encompasses a wide array of specialized plastics, including vinyl, nylon, polyester, and polyethylene. These materials exhibit impressive resilience, capable of withstanding temperature extremes ranging from a bone-chilling -40°C to a scorching +250°C. Moreover, they remain impervious to the corrosive effects of solvents, detergents, oil, grime, ultraviolet radiation, and even the corrosive forces of seawater. Polyester and polyethylene, in addition to their sturdiness, offer elasticity, enabling labels made from these materials to securely adhere to curved surfaces. Furthermore, non-plastic materials like aluminium can also be employed in this context.

This technology is notably well-suited for labelling heavy-duty equipment and freight containers. Moreover, it serves as an unalterable means of communicating hazard warnings or safety instructions. Labels capable of withstanding exceedingly high temperatures (up to 250°C) are typically applied to hot surfaces, including industrial machinery and furnaces.

The costs associated with these ultra-resilient labels typically fall within the realm of affordability. However, the specific materials chosen can influence the overall expenses.

2.2.3.2.6 Ultra-Destructible Labels

Ultra-destructible labels are ingeniously crafted from exceedingly delicate materials, frequently utilizing paper or PVC, and are fortified with remarkably strong adhesive. This combination yields a label that resists all efforts to be removed; any attempt to do so results in the label fragmenting into small, irremovable pieces. This intrinsic fragility makes ultra-destructible labels a highly effective anti-tampering measure. These labels come in a wide array of sizes, ensuring versatility in their application to various types of surfaces. Furthermore, they can be personalized and feature unique numbering. The greater the fragility of an ultra-destructible label, the more potent its anti-tampering properties. However, this fragility also translates to increased challenges when handling and applying the labels.

This category of label finds relevance in products protected by warranties, notably in domains like electronic equipment, and is equally embraced by service and repair centres as well as retail outlets. Additionally, these labels prove highly suitable for the food industry, where they serve as indicators of freshness on items such as jars.

The expenses associated with ultra-destructible labels typically remain budget-friendly, although the choice of materials employed can influence the overall cost.

Figure 27

2.2.3.2.7 Void Labels

Labels of this kind operate by leaving a mark on the product in the form of the word "void", custom text like "opened", or a designated logo. Consequently, when the label is removed, it imparts a visible sign of attempted tampering. Even if the message or logo is eradicated from the product, the same alert message will persist but appear in a negative format when the label is reapplied. The defining characteristic of void labels lies in their capacity to maintain the concealed status of the alert message or logo until the label is detached. Once the adhesive layer has been peeled from the object's surface, the label's integrity becomes irrevocably compromised, rendering any tampering evident.

Void labels find practical application in a variety of scenarios, including goods sold under warranty, leased items, and products undergoing service or repair, providing unequivocal evidence of unauthorized interference. Additionally, they serve as an effective means to oversee and regulate product integrity throughout the entire supply chain, extending from manufacturing to retail distribution.

The costs linked with void labels generally remain economical, although the extent of customization can influence the overall expenditure.

Figure 28

2.2.3.2.8 Tags

Tags can be fashioned from a range of materials and primarily serve the purpose of product identification. Nevertheless, their potential for bolstering brand protection expands, especially when paired with other technologies like RFID, specialty inks, or holograms. The effectiveness of product authentication using tags largely hinges on the secure attachment of the tag to the product. Consequently, their optimum functionality is achieved when used in conjunction with other security measures.

Tags offer an efficient means of product identification and substantiating authenticity, particularly when integrated with more advanced technologies such as holograms, RFID tags, optically variable inks (OVI), or tracer fibres. These tags are typically affixed to the product using durable threads, resilient nylon strings, or robust chains.

The cost associated with tags typically remains cost-effective, though it is contingent upon factors like material type, attachment methods, and the integration of additional technologies.

Figure 29

1.2.4.2 Laser Engraving

This cutting-edge technology employs a specialized laser to intricately etch closely spaced grooves of varying depths into a wide spectrum of surfaces and materials. Over these engravings, one can overlay images, logos, text, or identification codes, resulting in a fascinating play of colours when viewed from different angles. Often mistaken for holograms, these images prove exceedingly challenging to replicate. A prominent advantage of this technology is its inseparability from the product, rendering it a formidable deterrent against tampering. Three primary laser engraving techniques are in practice:

1. Annealing, also recognized as laser surface stamping, imparts markings onto ferrous metals and titanium by heating the surface, prompting oxidation underneath, and causing the metal to take on a distinct coloration within the marking's outline.
2. Real Laser Engraving involves the removal of material from the product's surface to form the marking. This method is particularly pertinent for metals, plastics, and ceramics.
3. Deep Laser Marking is a highly specialized approach, focusing on creating markings at precise depths within the product's surface, predominantly in metallic substrates.

Laser incisions are applicable to a wide range of materials, including paper, labels, leather, film, rubber, foam, wood, fabrics, PET, PVC, glass, stone, iron, nickel, steel, stainless steel, aluminium, and electrical components. This technology is notably utilized in the manufacturing of Italian identity cards (CIE).

It's important to note that laser engraving entails significant costs, although the specific expenses vary according to the context, material, and technique employed.

Figure 30

1.2.4.3 Anti-Alteration Devices

Anti-alteration mechanisms serve as a safeguard against unauthorized modifications to a product within its original packaging. While various specific devices could be designed for different types of goods, a prime example is the anti-topping-up or anti-refill cap. This ingenious contraption, often comprised of one or more diminutive spheres, is inserted into the neck of a bottle. Its function permits the outward flow of liquid from the bottle while effectively preventing any unauthorized topping up or refilling. This technology finds widespread application within the alcoholic beverage industry, chiefly in the protection of wines and spirits against counterfeiting.

Empty beverage containers designated for recycling often fall prey to interception, as they are refilled with inferior substitutes and subsequently marketed as the genuine, high-value product. Anti-alteration devices, particularly anti-refill caps, quash these deceptions by introducing one-way valves into the necks of bottles, making it impracticable to pour liquid back in.

Furthermore, anti-alteration mechanisms can be complemented by shrink sleeve labels adorning the caps and lids of bottles and jars. This additional layer of security acts as an extra barrier against tampering and illicit alterations. An illustrative example is presented in the accompanying image where an additional stopper is incorporated.

It proves challenging to provide a generalized estimation of the expenses linked to anti-alteration devices, as the costs are contingent upon the specific product and the specific device selected.

Figure 31

1.2.4.4 Seals

Seals encompass any mechanism designed to hermetically seal a package, safeguarding its contents against tampering. These seals may be fashioned from plastic or metal, and their complexity can range from straightforward and economical screw caps for bottles to more intricate designs. Installing and removing seals is generally straightforward, yet the level of security they provide largely hinges on the competence and discernment of the individual inspecting them. Mechanical seals, despite their diversity, share common attributes:

1. Their integrity relies on visual examination, requiring human verification.
2. They serve as a visual indicator of product security, immediately revealing any signs of tampering.
3. Unlike electronic seals, they do not record details concerning the time or location of tampering.
4. They lack the capability to autonomously assess their own integrity.

Seals are exceptionally adaptable and find utility across an extensive spectrum of packaging types, spanning diverse sectors. They even play a pivotal role in securing freight containers during transportation.

As seals are predominantly applied to the packaging rather than directly to the product, implementing this technology primarily impacts the wrapping and packaging stages, necessitating minimal modifications to the production process.

The costs tied to mechanical seals vary significantly due to their wide-ranging applications and adaptability. However, it can be noted that their expenses are substantially lower when compared to electronic seals.

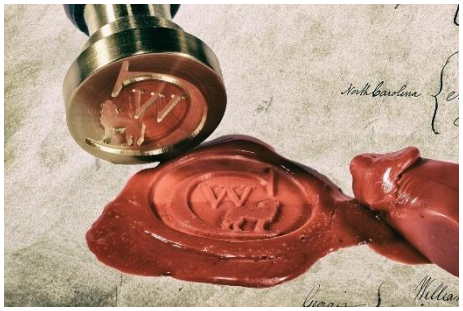


Figure 32

1.2.4.5 Security Threads

Security threads encompass threads crafted from a multitude of materials, including metal, fabric, and polymers, interwoven into, or otherwise affixed to products to facilitate authentication and counter tampering efforts. This technology's versatility allows for integration into a wide spectrum of products. Moreover, advanced security measures like specialized coatings or microprinting may be employed to enhance protection against counterfeiting. The various security threads can be categorized based on their materials and functions:

1. Metal threads, directly embedded within products to deter replication, often used in banknotes.
2. Miscellaneous threads, such as polypropylene and fabric, serve the purpose of attachment or sealing. They find utility in fastening tags to garments or products and act as micro-seals for warranty validation.
3. Polymeric threads come in various thicknesses and may include metal coatings (partial or complete), special light-sensitive pigment coatings, microprinted digits and text, and magnetization for concealed information detectable solely by magnetic readers.

Security threads are applied to secure products across a broad array of industries, with their most prevalent use being in banknotes.

When considering the integration of metal threads into your products, modifications to the production process are required to incorporate an embedding step. However, for other types of security threads used for tagging or printed information, no changes to the production process are necessary. These threads are typically applied to the final product or its packaging.

The diverse range of materials and application methods related to security threads makes it challenging to provide a comprehensive overview of the costs associated with their implementation.

1.2.4.6 Security Film

This innovative technology serves as a key safeguard for printed data on documents and packaging. Its primary function involves the application of a plastic film onto pages or other surfaces requiring protection,

accomplished through the application of pressure or heat. The plastic film is ingeniously imbued with specific security enhancements during its application, including tactile and colour elements that fortify its protective qualities.

There exist three prevalent methods used to infuse security measures into this film:

Beyond these standard techniques, there are more unconventional approaches, such as employing iridescent film, which dazzles with a pearlescent brilliance and exhibits a play of colours when observed from diverse angles. Additionally, the application of back-reflecting film renders it discernible through specialized viewing devices harnessing coaxial light.

1.2.5 Technologies for Digital Media

Digital media encompasses data presented in a format that can be comprehended by machines. This spans a broad spectrum of content, including digital images, videos, MP3 audio, e-books, video games, and databases. Anti-counterfeiting technologies tailored for digital media primarily revolve around techniques for embedding and verifying information within digital files, computer systems, and electronic devices. These technologies serve the dual purposes of safeguarding, identifying, and tracing the intellectual property content associated with these media assets.

The anti-counterfeiting technologies devised for digital media fall into four general types, encapsulated within two overarching categories: digital rights management (DRM) systems and automatic content recognition technologies.

DRM systems are strategically crafted to combat widespread counterfeiting of audiovisual works and are predominantly utilized by copyright holders and associated rights owners. These systems enable the safeguarding, enforcement, and administration of their rights in the digital domain.

Automatic content recognition technologies, on the other hand, primarily focus on identifying the content within media files or during playback on a device. These technologies fulfil a multitude of purposes, with safeguarding intellectual property standing out as just one facet of their utility. Automatic content recognition technologies that play a pivotal role in fortifying digital media against counterfeiting include digital watermarks, hashing, and fingerprinting. These techniques respectively encompass the incorporation, computation, and generation of information that is intrinsically linked to specific digital content, encompassing text, images, audio, and video. Subsequently, this information can be detected or extracted to ascertain the nature, origin, and source of the content.

1.2.5.1 DRM Systems

DRM systems exercise control over the access and utilization of digital content, a technology that has likely crossed paths with most individuals, often imperceptibly, due to the surging popularity of online streaming and gaming platforms. When streaming services impose restrictions on the number of devices per account, or

video game companies mandate the input of a product key for gameplay initiation, DRM systems are covertly in action, diligently safeguarding digital copyrighted materials. Their primary objective is to thwart the widespread unauthorized replication and distribution of digital copyrighted content through online channels. To achieve this, DRM systems employ two fundamental procedures that empower copyright holders and their affiliates to safeguard and regulate access to their digital assets:

1. Inclusion of Metadata: This technique entails embedding specific data (like the purchaser's name or account particulars) into the digital files. This data can only be discerned by designated software, adding an extra layer of protection.
2. Encryption: The digital content is rendered in a code that can solely be interpreted by devices or software equipped with an encryption key. The key can be distributed either offline or online, contingent on the authentication processes in place.

Through the encoding and encryption of digital files, DRM systems render these files immensely resistant to duplication outside of a managed environment. Furthermore, they enforce constraints on their usage, defining specific timeframes or designated purposes, all within the framework of the access licenses granted to end-users.

1.2.5.2 Digital Watermarks

Watermarks represent an ancient and enduring method of validation, steeped in a history that saw their original application on tangible objects, notably on paper currency. In the modern era, these time-honoured watermarks have seamlessly made the transition into the digital domain, manifesting in diverse forms. For instance, when you obtain a video from an on-demand streaming service, you may notice a personalized watermark embedded within, bearing your unique identifier. This digital watermark serves as a perpetual imprint of information within a digital file, effectively certifying its genuineness and origin.

The nature of information encapsulated in a digital watermark exhibits a remarkable variety. It can assume a visible form, like the distinct logo of a television channel gracing a corner of a video, or it may remain concealed, surreptitiously integrated by making imperceptible alterations in the pixel configuration of a specific video segment. Decoding such an invisible digital watermark necessitates the involvement of computer programs or specialized machinery.

Digital watermarks come in two discernible modes: private and public. A private watermark remains intelligible solely to individuals possessing the original, unmarked file or those equipped to unravel the watermark's meaning. In contrast, a public watermark is conspicuously evident and comprehensible, even to those unacquainted with the underlying content.

Furthermore, watermarks can be categorized as either fragile or robust. Their classification hinges on the degree of resilience to modifications in the data where they are embedded. Robust watermarks exhibit the capacity to substantiate ownership of a file or guarantee it, even in scenarios where the file's contents have undergone substantial changes.

The primary sphere of application for digital watermarks primarily revolves around the domain of multimedia content creation. Their role spans across a diverse range of mediums, encompassing DVDs, CDs, software, e-books, television programs, and, increasingly, throughout the expansive realm of online content. This domain encompasses audio, video, image files, texts, and documents, where digital watermarks serve as a steadfast guardian of authenticity and source verification.

1.2.5.3 Hashing

Hashing is a sophisticated computational technique hinging on a specialized algorithm, like MD5, SHA-1, or SHA-2, to craft a distinct marker, labelled as a "hash", that becomes intimately tied to a particular file, contingent upon its content. Remarkably, the hash assigned to two identical files will unfailingly mirror one another. In stark contrast, even the slightest disparity between two files, no matter how minute, ensures the generation of hashes that steadfastly differentiate from each other.

Within the expansive landscape of copyright protection, hashing emerges as a linchpin, as it furnishes the means to pinpoint and identify files that infringe upon copyrighted material. These errant files are then enlisted in "blacklists," constituting invaluable tools for cloud storage services. These services leverage the blacklists to effectively discern, obstruct, and subsequently expunge any unauthorized files. The overarching objective of hashing revolves around the nuanced capability to discriminate and demarcate myriad renditions of the same digital file.

This intricate process unfolds in a meticulous sequence. Commencing with the application of an algorithm, it confers upon the file a distinctive string of characters, christened as the "hash," which is thereafter securely ensconced within a designated hash repository. Subsequently, as a second digital file takes its rightful place, it traverses the identical hashing journey, culminating in the emergence of an associated hash. This newly minted hash is then subjected to a rigorous comparison with the pre-existing hash residing within the dedicated database. The outcome of this deliberative examination renders a definitive verdict: either the files are impeccably identical or diverge from one another in unequivocal terms.

1.2.5.4 Fingerprinting

Much akin to the distinctive traits of a human fingerprint, digital fingerprinting meticulously captures and records the one-of-a-kind identification characteristics inherent to a particular digital file. This innovative approach has found favour, particularly among video-sharing platforms, where content creators are granted the ability to digitally imprint their original videos. These digital fingerprints, in turn, find a safe haven within a reference database. Powered by specialized software, each novel or unfamiliar content undergoes a comprehensive analysis, resulting in the generation of corresponding fingerprints. These newly minted fingerprints are then meticulously cross-referenced against the extensive compendium of fingerprints housed within the database, with the aim of identifying matches and unearthing instances of illicit utilization.

The primary objective that steers the wheel of fingerprinting technology is centred around the realm of content recognition. It shuns any alteration or augmentation of the digital file's inherent content. Instead, fingerprinting methodologies delve into the examination of the distinct intrinsic attributes of a digital file,

which could encompass elements such as audio waveforms or video attributes. From this scrutiny emerges a unique string of values, encapsulating the essence of these properties, aptly referred to as the "fingerprint." These strings of values are meticulously logged and catalogued within a database, poised to be harnessed in the quest for uncovering resemblances and parallels with other third-party content that has also undergone the fingerprinting process. Notably, fingerprinting technologies exhibit a remarkable ability to identify not only direct matches but also akin and modified files, be it a recording of a film from a television screen or a reinterpretation of a musical composition.

1.2.6 Shared Ledger Technology (BLOCKCHAIN)

Strengthening your defences against counterfeiting can be achieved effectively by combining anti-counterfeiting technologies and tamper-resistant packaging with the use of shared ledger technology. This innovative approach provides a reliable means of tracking all transactions within a supply chain, from the initial production stages to the retail distribution. It operates on a decentralized peer-to-peer system, essentially serving as a database (ledger) that records verified asset exchanges simultaneously across all connected computers, free from the vulnerabilities associated with central server dependencies. Among the various shared ledger technologies, blockchain stands out as the most renowned.

The adoption of blockchain applications is a relatively recent development, gaining significant traction in recent years. While it was initially known for its role in financial transactions (with Bitcoin serving as a notable example), its adaptability extends to a wide range of markets. Businesses are actively exploring its applications in domains such as payment processing, digital identity verification, contract and dispute resolution, insurance, record-keeping, and enhancing the security of supply chains against disruptions and illicit activities.

One compelling feature of blockchain lies in its ability to eliminate the necessity for trust among the involved parties in a transaction, whether it pertains to financial dealings or the transportation of goods. Unlike traditional physical transactions that rely on mutual trust among all participants (including brand owners, manufacturers, carriers, logistics operators, distributors, and retailers in a supply chain), blockchain-based digital transactions occur swiftly, securely, and transparently through a "thrustless" mechanism, with no requirement for the parties to personally know or trust each other. Trust is embedded in the operation of the blockchain network, rendering explicit chains of trust or the presence of trusted intermediaries obsolete.

Blockchain technology functions as a 'shared ledger' system, where all the computers within the network, referred to as nodes, uphold identical copies of the ledger, essentially serving as a comprehensive transaction database. Each time a new transaction is added to the ledger, it is recorded in the copy of every participant. Every new transaction within a blockchain undergoes rigorous validation by all network participants and is secured with its own cryptographic hash (an encryption algorithm), creating a new block in the chain, thus giving rise to the term "blockchain." The decentralized nature of blockchain means that, beyond maintaining real-time duplicate ledger copies, each node within the system independently verifies every transaction before it becomes a new entry. Consequently, blockchain is not reliant on any single entity, be it internal or external, to oversee validation, monitoring, transaction reviews, or data alterations; these functions are collectively managed by the network. Each new block also embeds immutable encrypted data from the preceding block, ensuring a high degree of auditability for blockchain transactions. Since all data within a blockchain is shared

Politecnico di Torino

among all participants, anyone can scrutinize the records and their historical data at any time, rendering manipulation nearly impossible. In the event of a strong connection between physical products and digital transactions, blockchain can be harnessed for the meticulous tracking and tracing of a product's ownership and authentication history, early detection of counterfeits, and precise identification of their origins.

The "chain" aspect of blockchain hinges on a hash function, which is an algorithm that transforms transaction data into a fixed-length alphanumeric string, and this transformation is irreversible, making it exceedingly challenging to decipher. Once a new transaction is verified, the data is hashed. Each new block possesses its distinct hash and the unique hash of the preceding block, creating connections that form the chain. This characteristic simplifies the detection of any tampering within a blockchain, as a malevolent actor would need to alter the hash in the subsequent block to conceal their actions, necessitating the same alteration across all ledgers on all the nodes linked to the blockchain. Blockchain systems are categorized based on accessibility (public or private) and editability (permissioned or permission-less):

- Public permission-less blockchains enable anyone to participate in the network, allowing both reading and writing of data without requiring prior permission. These blockchains inherently prioritize transparency, as all actions on the network must be validated and visible to all participants, with actions hidden from some participants lacking proper validation. Public permissioned blockchains permit anyone to read the data but restrict the ability to write to selected participants.
- Private blockchains mandate permission for joining and participating in the network. Participants may be assigned varying read and write permissions, a feature particularly beneficial in sectors such as healthcare, where the need for preserving certain actions and data in confidentiality is imperative, while still benefiting from the security provided by a shared infrastructure.

Despite its relative novelty, blockchain is already in use within diverse anti-counterfeiting solutions. These solutions empower companies to establish their unique product IDs and oversee their supply chains. Although there isn't a single universal standard for leveraging blockchain in the battle against counterfeiting, examples of its application can be found across various industries, including luxury goods, diamonds, agri-food, electronics, and pharmaceuticals.

Let's delve into a practical example of implementing blockchain technology to bolster the security of a pharmaceutical supply chain. Within this framework, we have a network involving key participants, namely the manufacturer, packager, wholesaler, distributor, and doctor, each representing either a physical device, an individual, or an entity. These participants are assigned unique keys that designate their specific roles within the network, shielding their original identities and identifying them by these keys, such as "manufacturer" or "packager." The focal point of this chain comprises pharmaceutical products, regarded as the "assets." Each medicine receives an individual key or hash, which is then translated into a QR code affixed to the product. All transaction records find their repository in a chosen blockchain network, which could be one of several options available in the market, including Bitcoin Blockchain, Ethereum, Hyperledger, and BigchainDB. Once a transaction enters the blockchain, it becomes immutable, safeguarding the data from any alterations.

Participants in the network employ a mobile application to execute transactions through the blockchain. Upon the creation of a new pharmaceutical product, a unique hash or ID is generated and officially registered on

the blockchain. This registration designates the medicine as a digital asset within the blockchain network, with its hash serving as a tracking mechanism for its location and ownership throughout the network at any given moment. The transfer of pharmaceutical product ownership can be seamlessly conducted via the mobile app, resulting in various scenarios:

- The wholesaler procures a medicine from the manufacturer, and as the physical transfer unfolds, a corresponding transaction of the transfer is instantaneously documented on the blockchain.
- The wholesaler proceeds to vend the medicine to another wholesaler, distributor, or pharmacy, where the same transfer and registration procedure is applied.
- A doctor acquires the medicine from the pharmacy, employing the app to access the medicine's ID. By tracing its journey through the blockchain, from the manufacturer to the pharmacy, the doctor can validate whether the medicine is genuine or counterfeit. In the case of an authentic medicine, its complete product history is available, while counterfeit products exhibit no such record.

Estimating the comprehensive costs associated with deploying a production-scale commercial blockchain solution presents challenges, as these costs are intrinsically context-specific and contingent on the scale of implementation. Crucial factors that influence expenses encompass the selection of the blockchain network type (public or private), transaction volume, and data size. Additionally, it's worth noting that blockchain solutions demand a significant amount of energy to power their processing capabilities and performance, making them more energy-intensive compared to centralized peer-to-peer networks. Nevertheless, blockchain technology offers cost-saving advantages in other facets. By streamlining the secure execution of contracts and payments without the need for third-party intermediaries, blockchain eliminates the associated verification and transaction costs that are inherent in conventional physical contracting and payment procedures.

Figure 33

1.3 Examples From Varoius Markets

In this chapter I will introduces some strategies or additional measures introduces in specific sectors by governments or companies to protect even more their products and final customers. I will also present some financial data concerning counterfeit.

1.3.1 Pharmaceutical

The European Union has launched a system back in 2019, it was planned for 2016, to keep track of the medicines inside its borders and to control the imported one, all the countries members of the European union agreed plus 3 other states, Norway, Liechtenstein, and Iceland. This system is managed by the European Medicines Verification Organization (EMVO) which offers other services to help States or companies to implement and join this network. Each state member will have to create a National Medicines Verification Organization (NMVO) to manage the national archive which will be also integrated in the European systems. EMVO, EMVS and NMVO have been financed by private companies, in this case pharmaceutical manufacturers and importers while wholesalers and pharmacies contribute with the startup phase, they help to the creation of national entities and their governance. Member States will not participate with a financial contribute.

Since 2016 all medicines get an electronic passport, which is a unique two-dimensional bars identification code (Datamatrix 2D), a sort of machine-readable codes. When the European Medicines Verification Systems (EMVS) was launched it estimates to connect about 2 thousand pharmaceutical companies, 6 thousand wholesalers, 140 thousand pharmacies, 5 thousand hospital pharmacies and all the active dispensers or vending machines inside the UE borders. All the medicines which required a prescription will be entered and tracking inside the system to counter against counterfeit products, in this case these products are called also “Black-Pharma”. There will be special products that will be excluded from this network, these medicines are listed in a “white list” drafted by EU and every states will decide for themselves.

The European Union has also established that these information’s will be mandatory on/inside the identification code:

- Code, it will enable identification for pharmaceutical form, dosage, size, and type of packaging of the medicine.
- Number Sequence, no more than 20 characters which will be generated randomly by an algorithm.
- National Number, it identifies the product if required by the member state in which it will be sold.
- Lot Number.
- Expiration Date.

Some states, Italy, Belgium, and Greece have received an extension to “join” this network due the fact they already had a pre-existing system already working. Italy introduced a specific label to identify and keep track of the medicines and it also have implemented a Central Data Base to store data. The pharmaceutical label is a support on multi-layer adhesive paper produced by IPZS (Istituto Poligrafico Zecca dello Stato). In the database are stored all data referring to production and spreading of numbered labels posted on drug boxes which will enable to follow from production to purchase or the recoveries of the drugs inside the systems.

The major producers which export more than 70% of medicines in Italy declared, during 2019, that they already had updated their production line in case the Italian government decides to immediately adopt the European systems.

1.3.2 Banknotes

An example like the pharmaceutical markets is the one concerning current currency. There are different systems, worldwide or national that help the states to create a database to store data and simplify operation. In the European Union the central bank verifies and provides various services to the state members, such as the European Central Bank (BCE) which makes monetary policies and enforces them. There is also an informatic system which store data about counterfeiting, Counterfeit Monitoring System (CMS). Two institutions cooperate within the Bank of Italy:

- National Analysis Center (NAC) that has the task to analyze the banknotes suspected to be fake
- National Counterfeit Center (NCC) that coordinate all the "actors" of the system and to define the right to access to CMS

A global organization known as the Central Bank Counterfeit Deterrence Group (CBCDG) has a mission to explore prevalent and emerging threats to the security of banknotes and to propose solutions for implementation by issuing authorities, moreover the CBCDG supports and deploys technologies that deter the use of digital equipment to counterfeit currency. This group is formed by 35 central banks and note printing authorities organized at the request of the governors of the G10, an organization which contain the 10 most relevant economic powers. The banks inside the group are from the Canada, European Union, Japan, South Africa, Switzerland, and United States.

The technologies used to prevent counterfeiting are a combination of different methods. This choice to combine several methods was made to make the hardest possible to recreate fake currency. The most used is the marking technologies like security hologram, various inks (UV-IR sensitive), watermarks, microtexts and gulloche/rainbow printing. We can find all these technologies in every single banknote and most of these are visible to human the eyes by moving the banknote or by exposing it to the sun light, tasting it can also reveal important details.

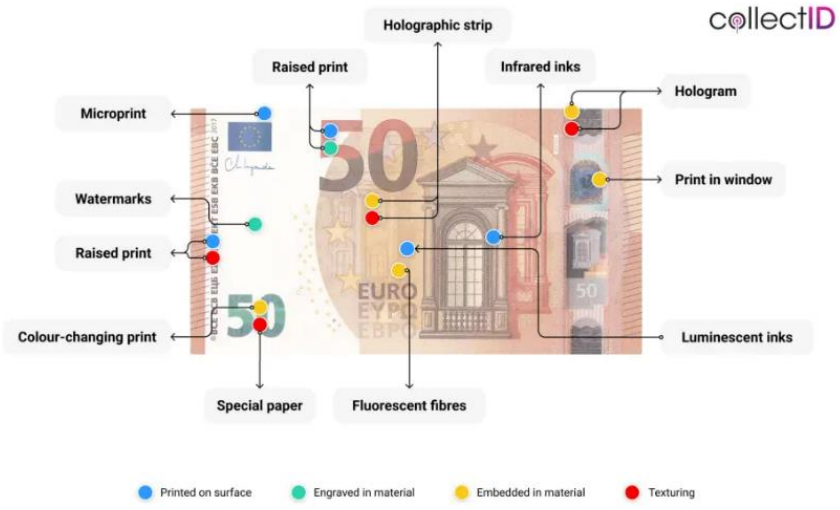


Figure 34

There are seven banknotes which are the same for all the member state, circulating in the euro zone. For this case has no sense to say that counterfeit measure must store or show some data such as the cigarettes solutions, the only purpose of these measures is to ensure the authenticity of the banknotes. On the forehead (recto) are shown windows and portals, while on the back (verso) is depicted a bridge inspired by the architectural style of different period in the history of European art.

We can identify the general and main characteristics for every cutting of banknotes:

1. The currency name written in Latin (EURO) and in Greek (EYPO).
2. The signature of Willem F. Duisenberg, the president of the European Central Bank (BCE).
3. The European flag.
4. The symbol "©" indicating the copyright protection.
5. The European Central Bank acronym written using the five official languages (BCE, ECB, EZB, EKT, EKP).

In addition to these common features, there are anti-counterfeiting solutions specific for every type (5, 10, 20, 50, 100, 200, 500 €).

Figure 35

1.3.3 Cigarettes

Cigarettes usually display machine-readable code on one side of the pack, this should prevent counterfeit products. In this case counterfeiting is increasing due to policy adopted by single member states which chose the price of a single pack. Inflation and the increasing of price could lead consumers to buy cheaper product even if they are fake and could be more dangerous. New generations products, such as electronic cigarettes, are amplify counterfeit because most of the parts are sold online through eCommerce. A phenomenon that is growing fast is the trade of the cigarettes called "Illicit Whites". These are in most cases legally produced in a country, but with the sole intention of being smuggled into other markets. Criminals often take advantage of vulnerabilities in Free Trade Zones (FTZs) to traffic those ones.

Smuggling and counterfeiting are affecting tax revenue by representing a loss since a fake pack represent that a legal pack is not sold. In 2021, in a report made by KPMG for PMI (Philip Morris Italia), was estimated that 10.4 billion euro were loss due to counterfeit. Another report made for "Il Sole 24 Ore", an Italian financial

journal, estimated that tax revenue loss was about 13.7% for traditional cigarettes and 12.8% for new generations products.

Concerning tobacco products there are several “laws” that regulate the information which must be shown or included on a package, applied based on the types of products. Member state of European Union assure that every single package should carry a unique identification code. To guarantee authenticity and integrity this code should be placed in a way that will be immovable, indestructible, indelible and should not be cover by any stamps or labels. These guidelines apply also for foreign product that are intended to be sold on European territory. The document which explains this guideline is DIRETTIVA 2014/40/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO of 3 April 2014. The unique identification code stores the following characteristics:

a) Date and place of manufacture.
b) Plant of manufacture.
c) The machine used for the production process.
d) The shift or the timetable in which the pack is manufactured.
e) The description of the product.
f) The market in which it will be sold.
g) The foreseen itinerary for transportation.
h) For foreign products, the Union importer.
i) The effective transportation itinerary which includes information about plant, date, destination, warehouse, recipient, point of departure.
j) Buyers’ identity from manufacturer to first retailer.
k) Invoice which includes all “financial” information through supply chain.

The letters a), b), c), d), e), f), g) and when possible, also h) are compulsory for the unique identification code. While for letters i), j), k) should be electronically accessible through the code. To write this unique code there are specific rules about symbols and characters that could be used, an example:

- LEITAv9h56cCx4yrENKY25v
- LEITAv9h56cCx4yrENKY25v19052017, which respect the previous one adds the timestamp.

Cigarettes and rolling tobacco must be marked as explained above from the 20 May 2019, while for other products such as electronic cigarettes or other that date will be the 20 May 2024. The products already on the market, without the unique code, before the 20 May 2019 could be sold until the 20 May 2020.

1.3.4 Food

One of the areas where counterfeiting is rapidly growing is the Food and Beverage market which is significant since the products denominated “Made in Italy” have seen a huge increase in demand. An article from 2022 estimates the value of counterfeit products is between 100-120 billion euros in the world due to the high

increase of demand for Italian products in the United States.There are 3 kinds of false product identified by the methods used to falsify them:

- "Classical", the original products are modified using different ingredients or through the combination of poor-quality elements with other like a bottle of whiskey made with a small amount of good whiskey and then other components.
- Alteration is the wrong application of some rules such as sell something after their expiration date.
- Italian Sounding is the adoption of name, noun or adjective that sounds Italian to let believe the consumer that these products are made in Italy.

The same article establish that "Italian sounding" in the United States has reached 40 billion euros, the 90% of Italian cheese is produced in American soil like Wisconsin or California. Coldiretti, that is the major association for representation and assistance for Italian agriculture, stated that more than 66% (2 out of 3) products are fake with an increase near to 70% in the last 10 years. Another business that grows most during Covid-19, is the eCommerce which generates around 24,5 billion of euro.

A lot of technologies anti-counterfeiting are used such as RFID, NFC, labels, seals (top of the wine bottle) or QR Code which assure a good protection but could also be altered. The main issue right now is that there is not a common database or standard rule to prevent counterfeiting, every player inside a supply chain use codes based on his decisions, need and logistics. There are laws regarding which information must be compulsory for food products as the Regulation (EU) No 1169/2011 that explain how and what information display on the package. These kinds of information fall into one of the following categories:

1. Information on the identity and composition, properties, or other characteristics of the food.
2. Information on the protection of consumer's health and the safe use of a food.
   2.1. Compositional attributes that may pose health risk for specific consumer groups.
   2.2. Factors related to durability, storage, and safe usage.
   2.3. The health implications, encompassing risks and consequences associated with harmful and hazardous aspects.

Unlike pharmaceutical or cigarettes products there are not mandatory information required. We can assume that all information regarding the production process, supply chain could help to fight against counterfeiting.

2. BENCHMARK

Now I will do an economic analysis of the automotive market and the technologies, strategy to prevent counterfeiting. It will be divided on two parts, in the first one I will look at the macroeconomic market illustrating what happens worldwide while in the second chapter I will analyze deeper some competitors to see how they respond to counterfeit and which solutions have adopted to do it.

2.2 Benchmark Automotive Sector

2.2.1 Introduction

The automotive sector has shown various problematics when counterfeit parts are entered in the market, such as:

- Recognition
- Safety
- Revenue
- Several trades point

When we talk about fake car parts, we have to consider that every vehicle is composed by an enormous number of components which could be copied and so recognition is more difficult due to the high level of "quality" for the reproduced elements and the high number of spare parts sold. Several players inside the market are conducting research/studies which demonstrate that various incidents are induce by fake parts, a commerce and industry body in India in 2018, put forward the data that 20% of car accidents in India are caused by counterfeit auto products.

In the last ten years, the challenges surrounding consumer protection have intensified in tandem with the surge in international transactions, the expansion of complex global supply chains, and the proliferation of online commerce. Consequently, the global movement of products has witnessed a substantial rise, leading to vulnerabilities in supply chains and exposing consumers directly to virtual marketplaces characterized by varying levels of quality and control safeguards. A study, commissioned by the International Chamber of Commerce's (ICC) Business Action to Stop Counterfeiting and Piracy (BASCAP) and the International Trademark Association, projects that the overall global economic impact of counterfeiting and piracy could reach $2.3 trillion by 2022. Some automotive parts may be short in supply due to logistics, manufacturing, or regulatory issues. In these cases, the counterfeiter's step in to leverage the demand and push fake parts onto the market. Fake parts distinction:

- There are replicas of actual vehicle parts which are made to look like the original.
- There are automotive parts that are smuggled from other countries through illicit channels and may not conform to the size or standard specifications for the vehicles in the country.
- There are salvaged parts from end-of-life vehicles or those damaged in accidents, fire, or flooding. These parts are severely compromised.

Counterfeiters hold the upper hand in producing and incorporating imitation parts that are virtually indistinguishable. Unless thoroughly tested, the counterfeit automotive sector proves to be more lucrative than the luxury industry. With the right resources and technology, counterfeiters can effortlessly scale up production at minimal costs, imposing significant expenses on brands and consumers alike. The market regarding anti-counterfeit technology, also the solutions applied on packaging, are forecasted to increase due to the technology evolution, high demand of products on eCommerce.

Since find reliable, recent, and specific data about automotive counterfeits parts I tried to do an analysis of the environment in which fraudsters could be proliferating.

2.2.2 Revenue

The shadow of counterfeiting looms ominously over the global economy, with staggering potential economic repercussions. An alarming projection by the World Trademark Review suggests that by the year 2022, the economic toll of counterfeiting could soar to a colossal $2.3 trillion. Among the various sectors affected, the automotive industry bears a substantial burden, as fake auto parts take a notable slice of this distressing pie. According to the Federal Trade Commission, the automotive realm grapples with an annual expenditure of $12 billion worldwide attributed to counterfeit parts, a striking $3 billion of which is shouldered by the United States alone.

The gravity of this issue becomes evident when we examine the statistics provided by the U.S. Customs and Border Protection. Over the course of a decade, from 2009 to 2019, there has been an astounding 86% surge in confiscated automotive parts, surging from 14,841 to a staggering 27,599. The domestic value of these items has experienced an even more astonishing uptick, ballooning by a mind-boggling 497% from $260.7 million to an eye-popping $1.56 billion.

The looming spectre of counterfeits casts its sinister influence over the supply chains of legitimate automotive manufacturers. Each year, these manufacturers grapple with monumental financial losses, eclipsing the $2 billion mark, arising from the sale of counterfeit tires and batteries.

Regrettably, the automotive industry is no exception to this growing epidemic, as counterfeiters relentlessly churn out bogus parts with impunity. Despite commendable efforts by national governments and industry actors like the UK Intellectual Property Office, the scourge of counterfeit auto components continues to spread its wings. The primary driver behind this malicious enterprise is the allure of easy profits, for counterfeit automotive parts prove to be an extraordinarily lucrative business.

The European Office of Intellectual Property (EUIPO) has gauged the staggering scale of losses inflicted upon the legitimate parts industry. A staggering €2.2 billion evaporates annually due to counterfeit tire sales, while counterfeit battery sales drain an additional €180 million each year. This dire situation creates a conundrum for consumers and professional mechanics alike, as distinguishing between a counterfeit and an authentic part becomes a formidable challenge, often thwarted by the clever packaging and deceptive appearances of these bogus components.

Moreover, it is crucial to recognize that this predicament extends beyond tires and batteries. An array of automotive parts regularly falls victim to rampant counterfeiting, including airbags, vital engine, and drivetrain components such as spark plugs, oil filters, and air filters, brake pads, automotive body components, electrical elements, wheels, and windscreens.

The onset of the COVID-19 crisis has also cast a lingering shadow on the counterfeiting market in Italy. In the tumultuous year of 2020, the total revenue for the Italian market was estimated at approximately €6.319 million, reflecting a modest decline from the previous year. The pandemic and its accompanying restrictions played a role in this downturn. Within this economic context, the expense attributable to counterfeit spare parts amounted to around €79 million.

2.2.2.1 Automotive Anti-Counterfeiting Council

Formed in 2015, incorporated as a non-profit 501 (c)(6) corporation in 2016, the automotive anti-counterfeiting council is an automotive association composed of representatives from North America vehicle manufacturers. The purpose of this council is to foster collaboration among automakers and their partners, working towards the eradication of counterfeit automotive components that pose a threat to U.S. consumers.

Using recent data from the Organization for Economic Cooperation and Development (OECD) the estimated financial impact of counterfeit auto parts entering the US exceeds $1 billion for A2C2 members. American consumers also continue to increase their online shopping. The US Department of Commerce reports eCommerce accounted for $149.7 billion in 2009, just 4.0% of all US retail sales, but in 2019 online sales had quadrupled to $595.5 billion that was a 10.9% of retail sales. Aided further by the COVID-19 pandemic, eCommerce has accounted for 14.0% off all retail through Q3-2020.

A2c2 has worked with governmental institutions to improve the situation and help car manufacturer. Drawing on these initiatives, 17 U.S. states have enacted legislation addressing the issue of counterfeit airbags. In 2018, in partnership with Interpol, A2C2 issued its inaugural "orange notice" related to the automotive sector, designed for use by law enforcement. This notice serves as an alert about a looming threat to public safety arising from counterfeit parts. It also published an infographic to illustrate and explain which part are counterfeited and how they could be dangerous to consumers.

eCommerce platforms have become particularly vulnerable to highly organized criminal enterprises and so A2C2 has also met representatives from Alibaba, Amazon, and eBay to express its concerns over the listing, sale, and shipment of counterfeit airbags in addition to other restraint system components. Alibaba has since introduced an automotive parts policy and announced a ban on listing airbags and related components.

Similar to this initiative there have been some governments which implemented new policies against counterfeiting. In a collaborative effort, the UK government partnered with the automotive industry and a trading platform to initiate a consumer-awareness campaign highlighting the risks associated with counterfeit automotive parts. Following this, the UK Intellectual Property Office provided guidance to consumers on methods to steer clear of purchasing counterfeit automotive components. In the Middle East, the UAE's Emirates Authority for Standardization and Metrology has put in place a system to stop automotive parts without its quality mark from entering the UAE. Traders have been instructed to remove non-compliant parts available in the market and a database containing information all about all the spare parts in the country, either manufactured there or imported, will also be developed.

2.2.3 Market Structure

The automotive sector is a multifaceted landscape, encompassing a diverse array of entities offering a wide range of services and products. While car manufacturers form a significant part of this sector, there are other crucial players, including those specializing in providing spare parts to both car manufacturers and end consumers. Within this intricate ecosystem, the concept of an Original Equipment Manufacturer (OEM) takes centre stage. An OEM represents a company whose products serve as integral components within the offerings of another enterprise, known as a Value-Added Reseller (VAR). The collaboration between the OEM and VAR is a symbiotic relationship, with the OEM often customizing its designs to align with the specific needs and requirements of the VAR. In essence, OEMs manufacture parts and components that are subsequently sold to VARs. It's worth noting that while some OEMs may produce complete products for VARs to market, they typically don't dictate the final configuration of the end product. For instance, an OEM might be responsible for crafting electronic components that are integrated into the HDTVs produced by a VAR like Samsung. In another context, an OEM could specialize in creating custom fasteners adorned with the branded monogram "RL" for Ralph Lauren. In the realm of traditional business practices, OEMs primarily focus on conducting business-to-business transactions, while VARs target the broader public or end-users.

One critical application of OEMs in the automotive sector involves the production of essential car components. These OEMs are responsible for crafting key elements such as exhaust systems and brake cylinders, which are subsequently integrated into the vehicles that roll off the assembly lines of car manufacturers.

2.2.3.1 Ecommerce

eCommerce platforms like Amazon, Alibaba, and eBay (specifically eBay Motors) have actively addressed the issue of counterfeit automotive products by implementing rigorous verification policies for listing products on their sites. Amazon's policies, in particular, serve as a robust example of the stringent regulations that online marketplaces should adopt to combat counterfeiting.

eCommerce started their business long time ago, but we have seen a huge increase the years previous COVID-19 and during it even more, a phenomenon that changed perspective and options to consumers for buying products in every class of goods. In the US online revenue for automotive parts will reach $41 billion in 2023, with a CAGR of 9% through 2025. We can identify two kinds of sellers:

- 1P (first parties) that sell directly.
- 3P (third parties) which use another platform to sell their product like Amazon or eBay.

This graph shows 2022 revenue projected at $19.8 billion and by 2030 it is projected at $35 billion, taken from a report on Hedges Company.

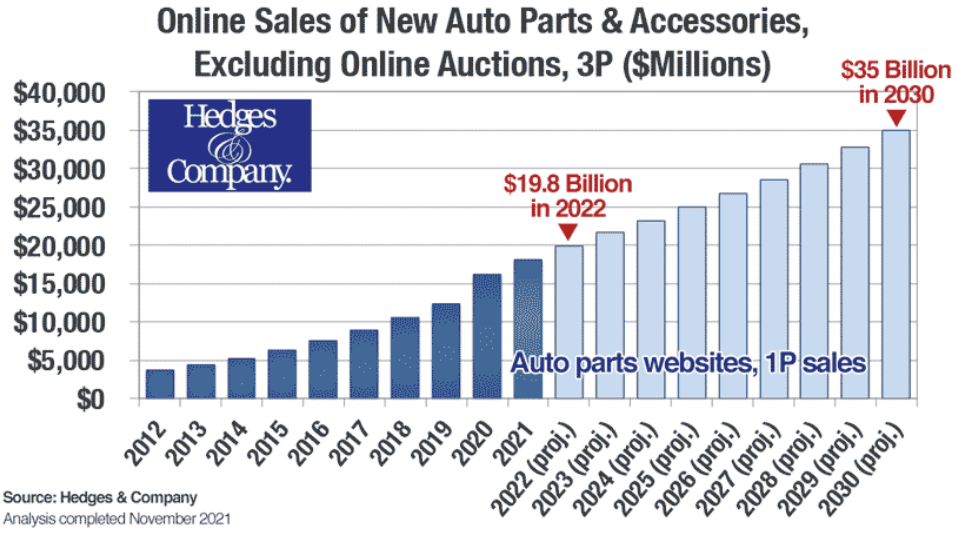


Figure 36

3P sellers use marketplaces such as Amazon, eBay, or Walmart to sell their goods, these marketplaces collect a fee in exchange for listing and selling a product on their platform. These sellers will generate a revenue around 18.3$ billion in 2022 and around $32.1 billion 2030. The forecast revenue, combining first parties and third parties seller, is around 67$ billion in 2030.

2.2.3.2 Aftermarket

The automotive aftermarket is a dynamic ecosystem that goes beyond the mere provision of replacement parts, accessories, and equipment for vehicle maintenance. It encompasses a broad spectrum of activities, including manufacturing, remanufacturing, distribution, retailing, and installation, all related to vehicles once they've left the factory premises.

While Original Equipment Manufacturers (OEMs) are responsible for producing the original parts used in vehicles, the automotive aftermarket steps in when a consumer needs a replacement. It is essentially the secondary parts market within the automotive industry, focusing on the entire lifecycle of vehicle components, chemicals, equipment, and accessories. This market comes into play after the original sale of the automobile by the OEM to the end consumer. It's worth noting that the components, accessories, and related products available in the aftermarket may or may not be manufactured by the OEM.

The automotive aftermarket caters to various needs, including replacement parts, collision-related components, items for enhancing appearance, and those designed to improve performance. It offers a wide array of products with varying qualities and price points, catering to almost all vehicle makes and models. Consumers have the flexibility to choose between repairing their vehicles independently (in the "do-it-yourself" or "DIY" segment) or seeking professional repair services (in the "do-it-for-me" or "DIFM" segment). This flexibility empowers consumers to decide where they want their vehicles serviced, maintained, or customized.

In recent years, the global automotive aftermarket industry has exhibited robust growth. Its value reached $392.35 billion in 2020, surged to $406.32 billion in 2021, and continued to grow to $427.51 billion in 2022, as reported by organizations like Grand View Research, Allied Market Research, Fortune Business Insights, and Straits Research. Projections indicate that this industry is poised for further expansion, with an anticipated valuation of $529.88 billion in 2028 and $551.92 billion in 2030. This growth trajectory corresponds to a compound annual growth rate (CAGR) estimated to fall between 3.8% and 4%.

Several factors contribute to this growth trend. Increasing consumer awareness about the importance of vehicle maintenance and repair for preserving efficiency and performance plays a pivotal role. The rise in demand for crossover vehicles and extended road trips is expected to boost the frequency of vehicle component servicing and replacement. Moreover, the desire for vehicle customization is emerging as a key driver in this thriving automotive aftermarket landscape.

2.2.3.2.1 Digitalization

The eCommerce industry has witnessed growth due to the unavailability of products domestically, affordable costs, consumer-focused targeting by market players, and higher quality of goods. Moreover, eCommerce offers a lot of advantages for SMEs to expand their business and become multinational and presents an opportunity for OEMs to sell their products directly to consumers, relieving them from the complex supply chain. Suppliers, OEMs, distributors, and workshop chains are progressively expanding their online presence. By simplifying the distributor layer and removing intermediaries, suppliers can achieve significant margins and cost savings that can be transferred to end-users. Digital platforms, including social media, are gaining increasing influence in customer research and the purchasing process across developed and emerging markets. Online sales channels provide customers with rapid access to information about part prices, enabling end customers to make informed decisions about which car parts to purchase. Growing digital service adoption index in the emerging country will boosts the use of eCommerce logistics market globally. Digital service adoption index is a global index measuring every country’s digital adoption across all industry verticals, such as government, business, and people. As an example, prominent component suppliers in the market, including entities like US Auto Parts Network, Inc. and CarParts.com, are poised to significantly influence global market demand in the future. The mentioned online aftermarket business platforms hold substantial potential in emerging economies, thanks to the trade gateways mentioned earlier.

Ecommerce players have made use of digital transformation to increase their footprint in their respective markets. Ecommerce breaks down geographic barriers for companies and allows sales in places that can be challenging to reach with traditional models, owing to which the automotive OEMs and component manufacturers across the globe are shifting their focus on online sales channels. Companies are increasingly transitioning to digital platforms to enhance customer experiences. In January 2020, Continental AG unveiled an online portal consolidating its services and product information for the market. The market's value chain consists of automotive replacement part suppliers and service enablers, fostering value exchange across various stages in the automotive sector. The digitization of global automotive component sales promises to address availability issues by providing access to a comprehensive range of components and streamlining transactions. This digital shift is expected to have a significant impact on the industry, driven by the growing preference for Internet-of-Things (IoT) and digitalization trends. Technological advancements in propulsion create opportunities in the market but concerns about high R&D expenditures may impede growth. While

automobile manufacturers face constraints such as production costs, certain aftermarket parts like filters offer the flexibility to choose components that suit specific operating conditions.

For instance, in October 2020 Bosch Rexroth launched a new eCommerce portal designed to provide the easiest access to select authorized Bosch Rexroth products, with the ability for customers to buy products with a credit card and schedule fast delivery.

2.2.3.2.2 Replacements Parts

The realm of aftermarket replacement part suppliers encompasses a diverse array of players, including those specializing in accessories, lubricants, tire supplies, and various component replacement solutions. Their role is vital in ensuring the continued operation and maintenance of vehicles.

In the year 2020, the segments of wheels and tires took centre stage, collectively contributing significantly to the industry's revenue. Notably, the tire segment emerged as the leader in terms of replacement parts, and it is expected to maintain its dominance in the market. This projected supremacy is attributed to the relatively shorter replacement cycle of tires compared to their component counterparts. Additionally, the filter segment is poised to experience a steady growth rate of over 3% due to expanding market penetration and increasing consumer awareness concerning the replacement and presence of cabin air filters. Notably, consumers in well-developed regions are showing a growing interest in high-value filter products, influenced by factors like emissions regulations and environmental consciousness.

Anticipated growth in the lighting components sector is particularly evident in regions marked by insufficient road infrastructure. The expansion of this segment is propelled by the adoption of advanced lighting solutions. In the case of brake pads, periodic product replacement is a driving factor, emphasizing the critical role they play in ensuring vehicle safety. Disc brakes, known for their ability to reduce stopping distances, are a significant growth driver within this segment.

The battery segment is projected to display steady growth, largely driven by strict government regulations and emission standards governing the automotive industry. Additionally, the value chain of this industry comprises service enablers, including providers of repair services and entertainment services. An interesting trend within the automobile industry is the increasing demand for hybrid electric cars. This trend is expected to impact exhaust parts and specific tools for these specialized vehicles. The rising cost of gasoline and petrol-based vehicles is a contributing factor to this shift.

Growth in disposable income among consumers in developing nations, such as China and Brazil, is anticipated to have a positive influence on market expansion. The surge in demand for locomotives is expected to boost the sales of automobile components. Across the globe, stringent regulatory standards related to car safety are expected to stimulate economic growth within the industry. The adoption of modern-age production technologies, such as 3D printing for automotive parts, is becoming increasingly prevalent among industry leaders. This deployment serves to optimize production costs, enhance fabrication efficiency, and reduce emissions, ultimately contributing to a more sustainable and eco-friendly production process.

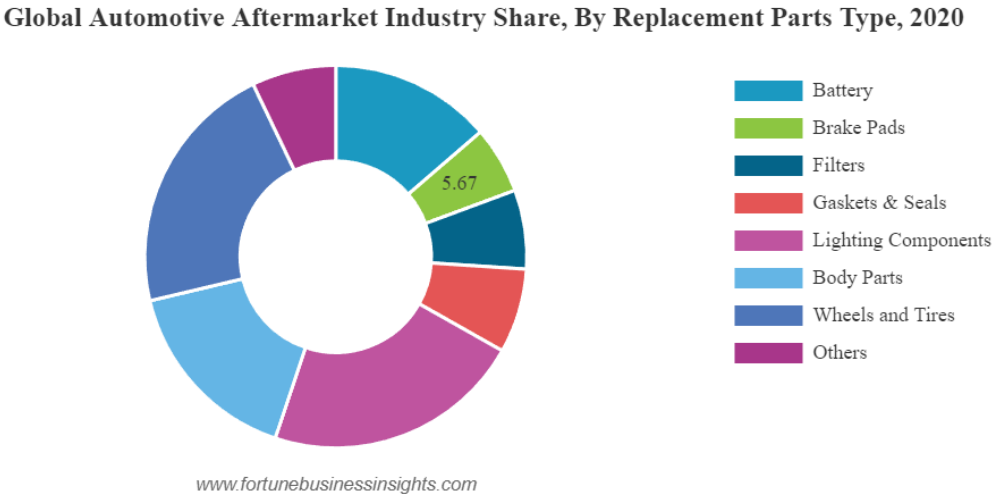


Figure 37

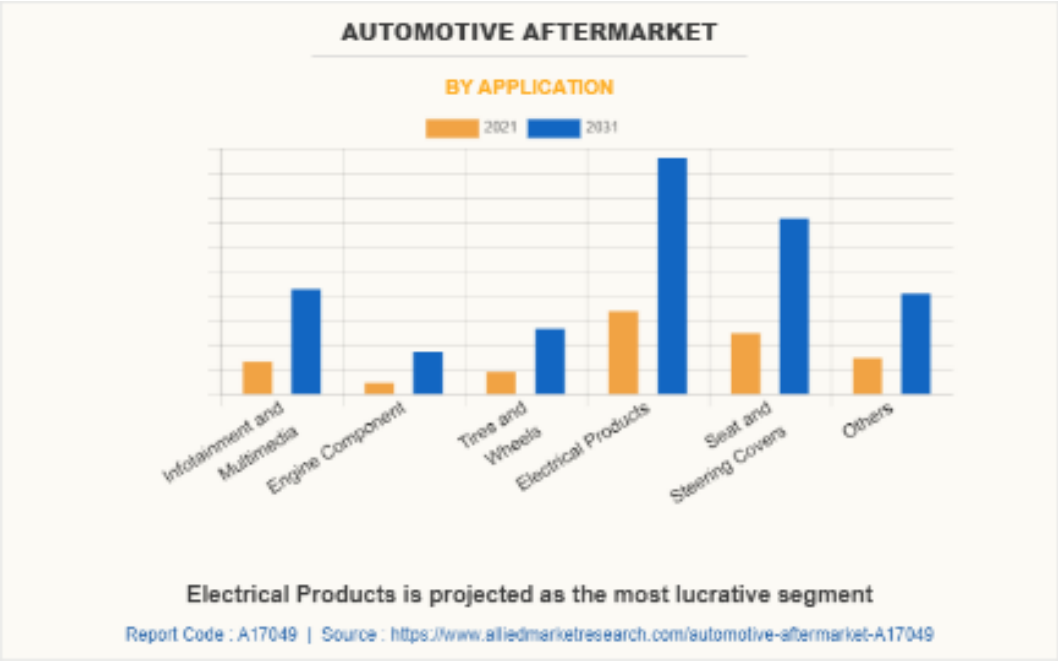


Figure 38

2.2.3.2.3 Distribution Channels

In 2022, the retail segment secured a commanding market share of 56.0%, establishing itself as the largest segment in terms of market size. This dominance is foreseen to persist, with the retail segment projected to maintain a substantial share in the market by 2030. Conversely, the Wholesale & distribution segment is poised for accelerated revenue growth from 2023 to 2030. The automotive aftermarket assumes a pivotal role in the holistic automotive manufacturing and maintenance framework, ensuring the timely replacement

of components to uphold vehicle performance standards. The market is currently undergoing a transformative phase propelled by the escalating impact of technological advancements, fostering a transition towards digitalization. A notable evolution is witnessed in the online aftermarket, where the sale of parts and services is increasingly shifting to digital platforms. This paradigm shift is compelling stakeholders across the value chain, encompassing Original Equipment Manufacturers (OEMs), Original Equipment Suppliers (OESs), wholesalers, insurers, and workshops, to align with the burgeoning trend of the online aftermarket. Key drivers for market growth include advancements in technology within auto parts manufacturing, an upswing in consumer and passenger automobile production, and the ongoing digitization of automotive repair and maintenance services, all poised to propel market expansion throughout the forecast period.

2.2.3.2.4 Service Channels

The landscape of the automotive market is marked by distinct segments, each wielding its share of influence. At the forefront, the original equipment (OE) segment emerged as a dominant force, asserting its presence with a commanding 71.1% share in 2022. Forecasts paint a picture where the OE segment continues to reign supreme in the aftermarket domain, maintaining its stronghold in terms of sheer size well into 2030.

Within the spectrum of customer segments, the "do-it-yourself" (DIY) sector is poised for dynamic growth, set to experience an upswing in revenue from 2023 to 2030. DIY customers are characterized by their technical expertise and enthusiasm for personally tending to the maintenance, repair, and enhancement of their vehicles. On the flip side, the "do-it-for-me" (DIFM) customers opt for a different approach. They acquire parts online but delegate the installation to professional workshops, a testament to the evolving landscape of automotive care.

The aftermarket service channel encompasses a diverse array of players, ranging from raw material suppliers to tier 1 distributors, automobile exhaust hubs, and manufacturing units. It also includes a vital network of aftermarket units, featuring jobbers who serve as intermediaries, culminating in the repair shops themselves. Among these components, repair centres stand out as pivotal stakeholders in the service channel.

A significant trend within the industry is the notable increase in strategic alliances and partnerships between collision repair centres and major auto insurance companies. This collaborative synergy is geared towards achieving a competitive advantage and securing a substantial market share. Prominent entities like Utica Mutual Insurance Company, State Farm Mutual Automobile Insurance Company, and Progressive Casualty Insurance Company have forged alliances with certified automotive repair shops across all U.S. states, underscoring the dynamic and evolving nature of the industry.

2.2.3.2.5 Expansion OEMs

Original equipment manufacturers (OEMs) have significantly elevated their engagement and emphasis within the automotive parts aftermarket value chain. They are establishing networks of non-brand-specific repair shops, expanding their presence to align with the evolving market driven by vehicle age. Leading market players, in response to this vehicle-age-driven trend, are introducing alternative service formats and second brands (as seen with Volkswagen's creation of VW Direkt Express) or incorporating remanufactured parts.

These strategic moves are aimed at competing with independent aftermarket players and retaining customers within their networks for extended periods.

OEMs are also channelling investments into enhancing customer experience and introducing distinctive aftermarket services by leveraging vehicle connectivity. This approach enables them to retain customers, automate decision-making processes related to service and repair, and stay at the forefront of technological advancements.

In the context of this industry shift, the French automaker PSA has strategically integrated the independent automotive aftermarket into its "Push to Pass five-year" growth strategy. Through a series of acquisitions, PSA has acquired stakes in key entities such as the distribution network Distrigo, Mister Auto, Aramisauto, and Autobutler. This comprehensive approach allows PSA to target a broad spectrum of consumers, irrespective of their vehicle brand, age, or distribution channel.

The market is also influenced by the growing awareness among customers about the importance of proper vehicle repair and maintenance for sustained efficiency and performance. Furthermore, the increasing demand for crossover and long-distance travel vehicles contributes to the need for periodic repairs and parts replacement. The evolving flexibility in vehicle design and production, enabling greater customer customization, is expected to be a driving force behind market growth.

2.2.3.2.6 Certification

When delving into the realm of market dimensions, a defining feature comes to the fore: the genuine parts segment. It reigns supreme with a substantial 51.8% share in the year 2022, wielding its influence within the aftermarket sector. As we cast our gaze forward, this genuine segment displays unwavering strength, destined to maintain its dominance in terms of sheer size, projecting its influence well into the horizon of 2030.

In the same arena, an exciting contender arises, poised for a remarkable ascent in revenue from the year 2023 to 2030. This is the uncertified segment, marking its presence on the stage. Counterfeit parts, tainted by their illicit origins, loom beyond the boundaries of legality. They shun the crucible of rigorous testing or official certification, and warranties are conspicuously absent from their offerings.

Conversely, the realm of genuine parts paints a different picture. Here, authenticity is paramount, with components either birthed by the car manufacturers themselves or sourced from Original Equipment Manufacturers (OEMs), often functioning as subcontractors. Genuine replacement parts bear the hallmark of quality assurance, presenting a diverse array that's conveniently accessible and buttressed by warranties. Alas, these merits are counterbalanced by the price tag, which often stands as a barrier, necessitating procurement through authorized dealers.

Meanwhile, certified automotive parts undergo a meticulous vetting process under the watchful gaze of accredited organizations. Among these custodians of quality, the Certified Automotive Parts Association (CAPA) has been an unwavering guardian since its inception in 1987. CAPA orchestrates rigorous testing protocols, methodically validating and ensuring the quality and suitability of automotive replacement parts.

A noble endeavour rooted in collaboration, it sprung forth from the concerted efforts of automotive insurance companies, uniting to champion the quality of replacement parts embraced by collision repair establishments. Certified parts assume the mantle of a cost-effective alternative to their often-pricier genuine counterparts.

In the shadows of these segments, uncertified parts emerge, carving out a distinctive niche as an alternative to the original automotive components. While they may lack the official imprimatur of the car manufacturer, their allure lies in cost-efficiency. This alluring characteristic fuels their promising growth prospects in the forthcoming years.

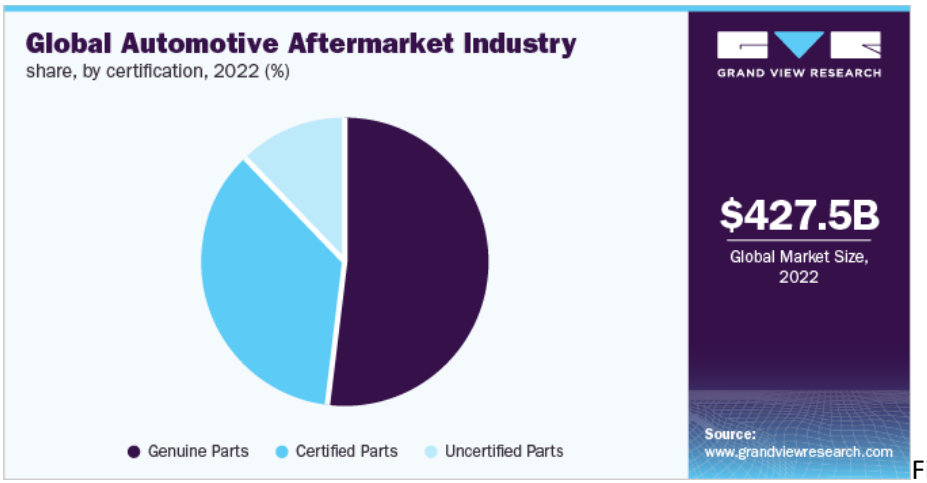


Figure 39

2.2.3.2.7 Vehicle Type

In the realm of market dynamics, the Asia Pacific region emerges as a dominant force, wielding a commanding 28.5% share in the year 2022. However, this market giant is not content with the status quo; it anticipates significant expansion from 2023 to 2030.

The driving factors propelling this ascendancy are multifaceted. At the forefront lies the seamless integration of cutting-edge technology into the fabrication of automotive components. This transformative shift ushers in an era marked by innovation and heightened efficiency. Simultaneously, a surge in consumer demand converges with increased production and sales of passenger automobiles, further fuelling the region's growth trajectory.

The digitalization of services related to automotive component delivery plays a pivotal role in shaping this landscape. It paves the way for enhanced convenience and accessibility for consumers, amplifying the region's market potential.

In this dynamic milieu, numerous companies adopt a strategic approach, setting their sights on acquisitions to fortify their position within the market. A notable instance is the acquisition orchestrated by the Goodyear Tire & Rubber Company in February 2021, when it joined forces with Cooper Tire & Rubber Company. This

synergy amalgamated their brand portfolios, thereby providing comprehensive services spanning the entire value spectrum of the market.

Concurrently, academic institutions and research and development organizations channel their efforts towards elevating the cost-efficiency and operational performance of pivotal automotive components. Their endeavours are geared towards cost reduction, ultimately translating into lower prices for end products. A noteworthy case in point is the innovative design crafted by a team of researchers affiliated with the Department of Chemical Engineering at Imperial College in London. This groundbreaking design achieves the remarkable feat of utilizing up to 80% fewer rare metals, thus delivering a significant reduction in the overall costs associated with vehicle and component manufacturing.

2.2.3.2.8 Key Players

The proliferation of advanced technology and an intensified focus on research and development initiatives, jointly undertaken by manufacturers and industry associations, stand as pivotal drivers behind the industry's anticipated growth. Within the dynamic landscape of the market, a myriad of local and regional competitors which are fighting for prominence, committed to delivering pioneering solutions that empower consumers to effectively navigate the ever-evolving terrain of technologies, security requisites, and business practices.

As the industry giants grapple for position, they teeter on the precipice of both opportunity and risk, with the competition for market share proving both advantageous and precarious. These leading players are strategically engaging in merger and acquisition activities, with the overarching objective of extending their global footprint and influence.

Prominent entities in the automotive aftermarket landscape include esteemed participants like 3M Company, Continental AG, Cooper Tire & Rubber Company, Delphi Automotive plc, Denso Corporation, Federal-Mogul Corporation, HELLA KGaA Hueck & Co., Robert Bosch GmbH, Valeo Group, and ZF Friedrichshafen AG.

2.2.3.3 Free Trade Zones

Another strategy frequently employed by counterfeiters and illicit trade networks involves the strategic utilization of free trade zones (FTZs). The enduring appeal of free trade zones can be attributed to the significant relaxation of regulations and oversight of operations within these zones. Essentially, governments abstain from imposing tariffs on the products being transacted.

Counterfeiters leverage the transit and transshipment of goods through a web of geographically dispersed free trade zones, all with the primary objective of concealing the illegitimate nature of their products. Once introduced into an FTZ, counterfeit goods can undergo a sequence of diverse economic operations. These operations encompass assembly, manufacturing, processing, warehousing, re-packaging, and re-labelling, among others. Upon the completion of these operations, the counterfeit goods can be either directly imported into the host nation for distribution or rerouted to another free trade zone, where the cycle of operations is replicated.

2.2.4 Packaging

A report from Maximize Market Research helps to understand the importance of the right packaging solution and how the market, cause a lot of companies are specializing packages to fight counterfeiting, is evolving due to eCommerce and online sellers.

The Anti-Counterfeit Automobile Packaging Market is poised to exhibit a robust growth trajectory, with a projected Compound Annual Growth Rate (CAGR) of 12.6% throughout the forecast period. The market is anticipated to reach a valuation of $271.18 billion by 2029, a significant surge from the $118.176 billion recorded in 2022. Anti-counterfeiting automobile packaging encompasses a diverse array of authentication management tools strategically employed to stay ahead of perpetrators and safeguard the automotive industry.

The escalating issue of counterfeit vehicle parts has resulted in substantial financial losses within the automotive sector. A noteworthy statistic reveals that over 60% of replicated automotive parts originate from China. The cumulative annual loss attributed to counterfeit parts in the automotive industry exceeds $55 billion, underscoring the urgent need for Anti-Counterfeiting Automobile Packaging. Currently, the aftermarket for auto parts is inundated with counterfeit products infiltrating the market at various junctures in the distribution chain.

Counterfeit parts entering the market through unauthorized channels pose significant challenges. Parts and services provided by non-authorized companies are typically not covered by vehicle warranties. In instances where performance failure occurs due to such parts, the accountability is often attributed to the automaker unless clear evidence suggests otherwise. These factors collectively drive the demand for global Anti-Counterfeiting Automobile Packaging as the automotive industry seeks robust solutions to mitigate financial losses and ensure the authenticity of vehicle components.

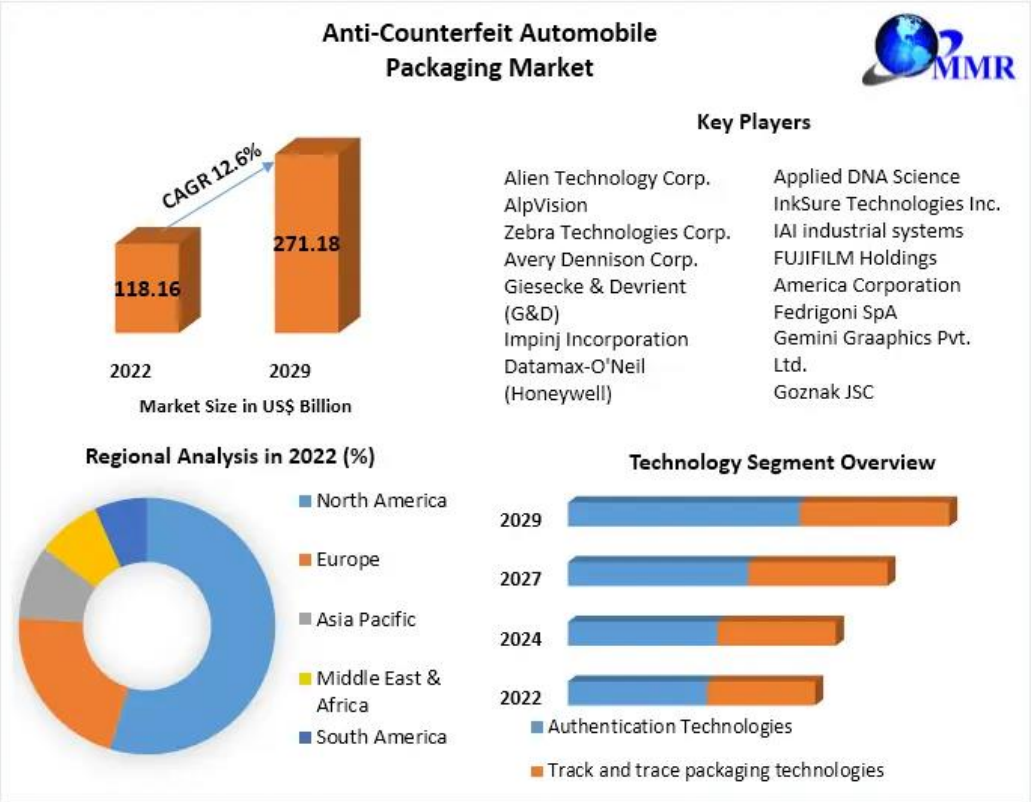


Figure 40

The continuous evolution of technology empowers counterfeiters to enhance their capabilities in replicating automotive parts and their packaging. What was once a conventional practice limited to rapidly moving maintenance items like filters and spark plugs has now expanded to encompass nearly every functional component, even extending to critical safety parts like airbags and sophisticated diagnostic equipment. This broader scope has not only facilitated the interchangeability of parts across various models but also rendered certain well-counterfeited components exceptionally enticing in terms of unit sales. The advent of new 3D AutoCAD software, rapid prototyping, and the ease of market entry granted by such technological advancements have collectively contributed to the escalating risk. This risk is expected to cast a shadow on the growth trajectory of the Global Anti-Counterfeiting Automobile Packaging Market.

Highlighting the magnitude of the issue, the U.S. Chamber of Commerce estimates that counterfeiting inflicts an annual cost of $150 billion to $200 billion upon U.S. businesses. This economic toll is directly correlated with the loss of over 650,000 American jobs. Meanwhile, the Federal Aviation Administration (FAA) projects that a staggering 4.2 million counterfeit parts find their way into the airline industry on a yearly basis. Disturbingly, some of these counterfeit automotive brake linings are constructed from materials as dubious as sawdust and cardboard, with profound safety implications that cannot be ignored.

The United States has intensified its focus on urban security, spurred by various factors. These developments are poised to contribute to the growth of the Global Anti-Counterfeiting Automobile Packaging Market within the region.

2.3 Analysis Competitors

In this part of the chapter, I will analyze some solutions adopted by the competitors. I have classified them in three class:

- Engine/Powertrain Manufacturer
- Supplier
- Supplier/Engine Manufacturer

Engine/Powertrain Manufacturer are those companies which have as their core business or as one of their core business the engine manufacturing. Supplier have been selected because I found very useful information on their website, this information is very easily to find for potential customers looking to understand the differences between a genuine and a fake goods (terms used for research: counterfeit, brand protection, genuine parts). Supplier/Engine Manufacturer are companies which could be identified as supplier for other companies or aftermarket, but they present a subsidiary or a “child” company which is specialized in the engine manufacturing.

2.3.1 Engine/Powertrain Manufacturer

2.3.1.1 Cummins

Cummins Inc. stands as a prominent American multinational corporation specializing in the design, manufacturing, and distribution of engines, filtration, and power generation products. Beyond product offerings, Cummins extends its services to encompass engines, fuel systems, controls, air handling, filtration, emission control, electrical power generation systems, and trucks. With its headquarters situated in Columbus, Indiana, Cummins boasts a global presence, reaching customers in around 190 countries and territories. This outreach is facilitated through an extensive network comprising over 600 company-owned and independent distributors, totalling approximately 7,200 points of distribution.

In a strategic initiative to fortify its components and spare parts supply chain against counterfeiting, Cummins Inc. has implemented a hologram protection labelling project in one of its global regions. This initiative enables customers to easily differentiate genuine products from counterfeits. As part of this endeavour, Cummins applies its original part number labels to all components supplied in the designated region, complemented by additional hologram protection labels. The transparent hologram, integrated into a printed base label, exhibits distinct properties, including slots along the edges and a QR-code. This multifaceted approach empowers customers to verify the authenticity of a part seamlessly.

Furthermore, Cummins' commitment to authentication extends to its Stamford AC generators, which bear holograms and unique machine reference numbers. These features enable both visual authentication and online verification of genuine items. The holograms, crafted using Du Pont's photopolymer, showcase vibrant red and green colours. Notably, when tilted forwards, three white spots appear above the word "Stamford," and when tilted backward, four white spots become visible underneath the same word, offering a reliable means of authentication. The company has also implemented a new label.

The figure below represents an example of how this hologram works, when moved it shows different number while when rotated the words “cummins” and “genuine” appear. At the end the customer could also enter the verification code on the Cummins portal. All these operations to check the product are provided by precise instructions on the portal.

Figure 41

2.3.1.2 Caterpillar

Caterpillar Inc. stands as a prominent American manufacturer specializing in construction, mining, and various engineering equipment. This corporate heavyweight holds the esteemed title of being the world's largest producer of construction machinery. The roots of Caterpillar Inc. can be traced back to the merger of two established entities in 1925: the Holt Manufacturing Company and the C.L. Best Tractor Company. This amalgamation gave birth to the new entity, known as the Caterpillar Tractor Company, hailing from the state of California. The preceding century had witnessed the formation of these two companies, each embarking on its own journey with the ebb and flow of events, particularly in the wake of World War I and World War II. These challenging times took their toll on these companies' financial stability. To overcome these difficulties, the financially robust C.L. Best decided to join forces with the dominant market player, Holt Caterpillar, in a strategic merger. Fast forward to 1986, and the company underwent a transformation, reorganizing itself as a Delaware corporation under the name we recognize today, Caterpillar Inc. In the fiscal year 2010, Caterpillar organized its products, services, and technologies into three primary lines of business, serving both private and governmental entities: machinery, engines, and financial products. However, as of 2022, Caterpillar has restructured its reporting framework, presenting its financial performance through four distinct business segments: construction industries, resource industries, energy & transportation, and financial products. This evolution reflects Caterpillar's strategic adaptation to changing market dynamics and its commitment to providing a more detailed and nuanced overview of its diverse business operations. One significant facet of

Caterpillar's operation involves the manufacturing of diesel and natural gas engines, along with gas turbines. These engines find application not only within Caterpillar's own vehicles but also as prime movers in locomotives, semi-trucks, marine vessels, ships, and they serve as power sources for peak-load power plants and emergency generators.

A pivotal moment in Caterpillar's history occurred in 1998 when it acquired Perkins from LucasVarity for a substantial sum of $1.325 billion, a move that created what was touted as the world's largest diesel engine manufacturer.

One cannot overlook the unmistakable presence of Caterpillar machinery and other company-branded products, identifiable by their signature "Caterpillar Yellow" livery and prominently adorned with the iconic "CAT" logo.

2.2.3.2.1 Perkins

Established in 1932 in Peterborough, England, Perkins Engines Company Limited has carved its niche as a prominent diesel engine manufacturer catering to diverse markets such as agriculture, construction, material handling, power generation, and industrial sectors. Over the years, Perkins has significantly expanded its engine catalogue, showcasing a diverse array of engine specifications, encompassing both diesel and petrol engines for automotive applications.

In the early 1970s, Perkins emerged as a key supplier to Caterpillar Inc., forging a strategic partnership where Perkins supplied smaller and mid-sized engines to Caterpillar, who, in turn, was a major producer of large diesel engines for various stationary and mobile applications.

Recognizing the critical importance of safeguarding its after-sales parts within the supply chain, Perkins Engines has incorporated tamper-evident hologram seals. This initiative plays a pivotal role in securing the authentication of its components. The British diesel engine company has been utilizing holograms on its packaging for an extended period, aligning with a robust brand protection strategy. To fortify this effort, Perkins engages in end-user education campaigns, particularly in international territories susceptible to counterfeiting activities. This comprehensive approach is further supported by the collaboration with OpSec, the hologram supplier, ensuring a resilient defence against counterfeiting threats.

On their site they declare that the hologram solution is your assurance that the parts you have bought have been manufactured by Perkins and that any parts without the hologram is not a genuine part and will not carry the 12 months Perkins standard warranty.

Furthermore, the hologram has been developed to minimize the risk of unauthorized reproduction, it has been tested and continues to be improved to ensure it is as tamper-proof as possible in the future too.

I quote an “highlighted” phrase on their website: Put simply, if your packaging does not have a Perkins hologram, it will not contain an authorized Perkins part.

Figure 42

2.3.1.3 Isuzu Motors

Isuzu Motors Ltd., a Japanese multinational automobile manufacturer headquartered in Yokohama, Kangawa Prefecture, Japan, is commonly recognized as Isuzu. Derived from the Isuzu River, the kanji characters of Isuzu signify "fifty bells." The company primarily engages in the production, marketing, and sale of commercial vehicles and diesel engines. Isuzu-branded vehicles have a global presence, being marketed and sold in commercial markets across the world. The core focus of Isuzu lies in commercial vehicles, particularly diesel-powered trucks, buses, and construction equipment.

In many parts of Asia and Africa, Isuzu has gained prominence for its diverse range of trucks, spanning various sizes. Notably, Isuzu transitioned away from the sales of sedans and compact cars in the late 1990s, redirecting its focus due to a decline in sales. During the period when Isuzu did offer passenger cars, their distinctiveness was marked by a dedicated emphasis on the diesel engine niche. As early as 1983, well before the surge in diesel sales, a significant 63.4% of Isuzu's passenger car production was attributed to diesel engines. During the 1990s Isuzu became the first manufacturer in the world for industrial vehicle (medium and heavy above 6.1 tons), reaching the greatest number of units sold in the 1996 in the United States. Isuzu was the first company to introduce the common rail system in off road vehicles. In December 1998, Isuzu received the prize “Technology of The Year” for the best engine produced in that year from Automotive Research’s Journalist Conference in Japan. In 2009, Isuzu withdrew from the consumer market in the United States citing insufficient sales. Historically, Isuzu has predominantly operated as a manufacturer of small to medium-sized compact automobiles and a diverse range of commercial trucks, spanning from medium-duty to larger sizes. However, the global market dynamics reveal varying demands, prompting Isuzu to adapt its market presence accordingly.

Diesel engines are one of the core businesses of Isuzu Motor and during the early 2000s they had over 15 million of engines produced on their plants, while in 2009 they produced almost 21 million of engines. Their running park is estimated to be over 20 million engines worldwide, the diesel power division, known as PowerTrain Division, in America is in Plymouth, Michigan.

Isuzu recognize the counterfeit parts as a huge issue for their customers and their sales, report/articles reported on their site highlighted how fast is increasing this phenomenon and how much revenue there are losing. For example, in Africa where they have the highest market share Isuzu estimated that almost 80% of spare parts acquired are fake. Isuzu advise to look carefully to:

- Part Number
- Cost
- Country of origin.

Isuzu recommend to always manually check the spare parts to notice if it fit properly or there are any differences between that and a genuine part. There are no references to solutions adopted on their products on their website.

2.3.1.4 Weichai Group

Weichai Holding Group Co. Ltd., commonly known as Weichai Group, stands as a Chinese state-owned enterprise specializing in the design, manufacturing, and sale of diesel engines. Operating across four distinct business sectors—engines and vehicles, powertrains, luxury yachts, and automotive parts—Weichai Group is headquartered in Weifang, Shandon Province, China. With a vast presence, the group encompasses over 80 subsidiaries, both within China and internationally.

Weichai Group's diverse portfolio includes offerings in commercial vehicles, construction machinery, marine power, agricultural machinery, and power generation. Additionally, the group, through its subsidiaries, extends its reach to provide transportation equipment, buses, luxury yachts, and hydraulic products. With a global footprint comprising more than 35 offices and 245 authorized service stations, Weichai products are distributed in approximately 110 countries.

The roots of Weichai can be traced back to its inception as Yucheng Ironworks (later renamed Coastal Ironworks) in 1946. Initially focused on the production of 79-type rifles and steamboat repairs, the company relocated to Weifang in 1948, venturing into the manufacture of 15 hp and 40 hp low-speed diesel engines. In a landmark development in 1953, Weichai successfully introduced the 6108 series diesel engine. Subsequently, the company underwent renationalization into the fourth Mechanical Industry Bureau under the Ministry of Machine-Building Industry and was rebranded as Weifang Diesel Engine Works. This marked the commencement of dedicated efforts in research, development, and production of diesel engines.

Weichai Power, a subsidiary established in 2002, forms a comprehensive industry chain encompassing power systems (engines, transmissions, and axles), heavy vehicles, automobile electronics, and parts. During 2005, they launched the Euro III “Landking” series engine, WP10 and WP12, which were China’s first Euro III diesel

engines. During the same year, the company acquired Torch Automobile Group allowing them to own heavy-duty trucks, transmissions, and axles.

On their site is present a page which explain how to check the security code used by the company. In order to verify the authenticity of purchased Weichai products, customers are required to follow a straightforward process. Initially, they need to scan the QR Code associated with "Weichai Mall" and subscribe to the WeChat Official account of the same. Subsequently, customers can perform a product authentication check by scanning the QR Code located on the upper left corner of the security label through the "product scanning code" feature. This ensures that the products in possession are genuine Weichai items. After the can phase it will be displayed if the product is genuine or counterfeited. In case or fake parts, the code could show to the user two messages:

- Exercise caution as the scanned product code is incorrect.
- Beware of potential counterfeiting risks as the scanned purchased code has been frequently accessed.

There is another QR Code under the red sign which give the customer the opportunity to win a prize if scanned.

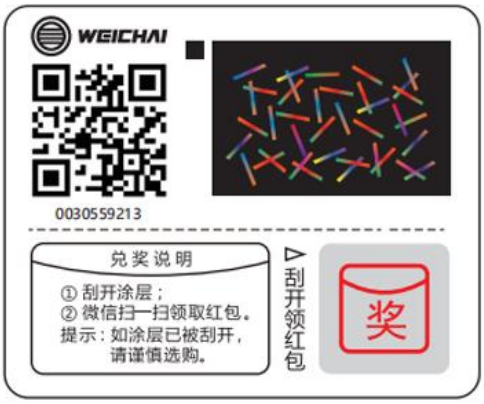


Figure 43

2.3.2 Supplier

2.3.2.1 Bosch

Founded by Robert Bosch in Stuttgart on November 15, 1886, Robert Bosch GmbH, commonly known as Bosch, stands as a German multinational engineering and technology company headquartered in Gerlingen, Germany. The majority of Bosch, 94%, is owned by the Robert Bosch Stiftung, a charitable institution with no voting rights, focusing on health and social causes unrelated to Bosch's business. Bosch operates in four main business sectors: mobility (hardware and software), consumer goods (including household appliances and power tools), industrial technology (drive and control), and energy and building technology. Renowned as the world's largest automotive supplier by revenue, Bosch has a rich history of innovation in the automotive industry. Shortly after its establishment, Bosch introduced a low-voltage magneto for gas engines in 1887. The

company furthered its impact by integrating magneto ignition devices into automobiles starting in 1897, establishing itself as a key ignition system supplier. In 1902, Bosch's Chief Engineer Gottlob Honold unveiled the high-voltage magneto ignition system with a spark plug. The 1920s marked Bosch's expansion into various automotive technology products essential for everyday car use, such as the electric horn (1921), windshield wipers (1926), and direction indicators ("trafficator," 1927). In that same year, Bosch also introduced injection pumps for diesel engines. After the collaboration regime Bosch had several years in which was struggling and only after some time, they were able to recover and produce spark plug for the Allies. At the beginning of the 1950 it introduced the petrol injection which became standard for car only decades later. One of the major innovations was the ABS, All Brake System launched in the 1978. One of the most famous innovations is the Common Rail launched in the 1997.

Bosch has integrated holographic technology to secure its products utilized in diesel engines and diesel fuel injection systems. The product packaging is affixed with secure code labels featuring hologram technology that is exceptionally challenging to replicate. Each label contains a unique 18-digit secure code, with the last six characters individually repeated within the hologram. When exposed to direct light, the code and logo shimmer in rainbow colours, while in indirect light, only black and silver structures are visible. Customers can visit a dedicated website link and enter the code for verification.

Traditional anti-counterfeiting solutions like scratch-off stickers and hologram labels have evident drawbacks. Scratch-off stickers are simplistic but not user-friendly, while hologram labels, though straightforward, tend to be expensive. Conventional QR codes are economical but susceptible to replication. Recognizing these challenges, Bosch Research in Shanghai initiated research on a more secure and user-friendly anti-counterfeiting solution integrating IoT and computer vision, termed the "Secure Product Fingerprint." Developed by Bosch China, this patented solution, grounded in computer vision and AI technologies, captures a unique fingerprint of a product and stores it in the cloud. The fingerprint can be either an assigned QR code enriched with micro-features (Artificial Fingerprint) or a snapshot of a specific area on the product's surface (Natural Fingerprint). Customers can use a smartphone to scan the QR code label or the designated area on the product, verifying authenticity by comparing it to the sample stored in the cloud. This can be accomplished through a dedicated app, WeChat, or a standard QR code scanner. Initiated in 2017, the project involved the development of algorithms and other intellectual properties on computer vision by Bosch Research in China. Following a market study on food safety conducted by the Business Development and Strategy department in the Bosch China headquarters, the project evolved into an integrated solution for anti-counterfeiting, track & trace, and Customer Relationship Management (CRM) tailored to local market needs. Multiple Minimum Viable Products (MVP) were created and tested internally to identify essential features. Then through a collaboration with Bosch Accelerator Program, Fudan University which contributed on algorithm development and market insights, BoschIOX for IoT full-stack development and commercialization. With those join effort, the project has gone through several remarkable milestones:

- 2017 Q4 set up of project team with Bosch Research and Bosch.IO
- 2018 Q4 1st proof of concept completed with internal customers.
- 2019 Q2 product launch.
- 2019 Q4 1st external customer acquired.
- 2020 Q1 breakthrough on natural fingerprint algorithm.

- 2020 Q3 1st natural fingerprint customer acquired.

The comprehensive Secure Product Fingerprint system integrates user interaction and a cloud server. Users leverage the Secure Product Fingerprint app or WeChat mini program to transmit data and receive results, while all fingerprint information and AI inference models are housed in the cloud. The app directs users to capture a high-quality snapshot of the fingerprint area. The image-processing algorithm extracts necessary fingerprint features and stores them on the cloud server. During verification, users utilize the app to capture the fingerprint of the product, allowing the AI inference model to ascertain consistency between the captured fingerprint and the original/registered one. The verification result is then accessible to the user within the app.

Currently are supported two kinds of fingerprints:

1. Artificial, based on existing QR code supplemented with a random micro-feature to ensure uniqueness and un-clonability.
2. Natural, recording the inherent surface texture of the product as its distinctive identification characteristic.

A crucial aspect of this system lies in its ability to amass more fingerprint data through end-user uploads, feeding this data into the computer vision machine learning model. This concept enables the learning of products through enhanced connectivity. Moreover, the Secure Product Fingerprint has the potential to enhance transparency in distribution channels for manufacturers. Leveraging the IoT architecture, manufacturers can track each product with a Secure Product Fingerprint throughout its entire lifecycle. Users can trace products through distribution channels to end customers and beyond, even including warranty service providers. This approach provides companies with insights into stock volumes, goods movements, and retailer performance. It streamlines recall procedures and notifies affected customers of faulty batches. All cloud-stored data can be utilized for in-depth data analysis to achieve improved Customer Relationship Management (CRM). To ensure the authenticity and integrity of Bosch products, specific Bosch packages feature authenticity seals. By scrutinizing these seals and entering a security code on the Bosch website, various partners and consumers can verify product authenticity at any given time. These two pictures are an example, used by Bosch to explain their labels.

Figure 44

Figure 45

2.3.2.2 AG Continental

Continental AG, headquartered in Hannover, Germany, is a German multinational company dedicated to the manufacturing of automotive parts, focusing on a wide range of products such as tires, brake systems, vehicle electronics, automotive safety, powertrain components, chassis components, tachographs, and more. The company operates across six divisions: Chassis and Safety, Powertrain, Interior, Tires, ContiTech, and ADAS (Advanced Driver Assistance Systems). Continental is the world's third largest automotive supplier and the fourth largest tire manufacturer.

The original packaging of Continental spare parts has helpful numbers, codes and icons that enable you to identify the parts inside quickly and confidently. On their site they explain how to identify spare parts (showed in the second picture below):

1. Short number and icon, fast orientation and product information.
2. Components and product name, overview of packaging information.
3. Make of vehicle, product suitable for specific automobile manufacturer.
4. MAPP code, this guarantees unique identification.
5. The tesa PrioSpot®, maximum counterfeit protection.

Subsequently, the company elucidates on the implemented solutions in points 4 and 5, considering them as the most reliable and pivotal. The utilization of tesa PrioSpot® technology, enriched with diverse security features, stands as a formidable safeguard ensuring maximum protection and facilitating the unequivocal identification of limitations. Each label is endowed with a unique code, incorporating the last four digits of the MAPP code, exhibiting a radiant iridescent display in rainbow colors when illuminated. This innovative label serves as an enhancement of the tesa Holospot®, crafted by the company "tesa." Continental's products also bear distinctive marks, with the trademark, part number, encoded batch number, and manufacturing date engraved into their brake drums, while other products boast their own distinctive identity marks.

An additional measure to deter counterfeit products involves the MAAP code, introducing additional security features through the incorporation of a data matrix code known as MAPP. The concluding characters of this code are likewise reflected in the Holospot® or PrioSpot®. Verification of this code can be easily conducted by manually entering it on the Continental website, providing prompt confirmation of the authenticity of the part. Example of a MAPP code:

(01)14006633314036

(21)94YZPG084C6S

You will have to enter the second line of the MAPP code without the preceding “(21)” on the specific field.

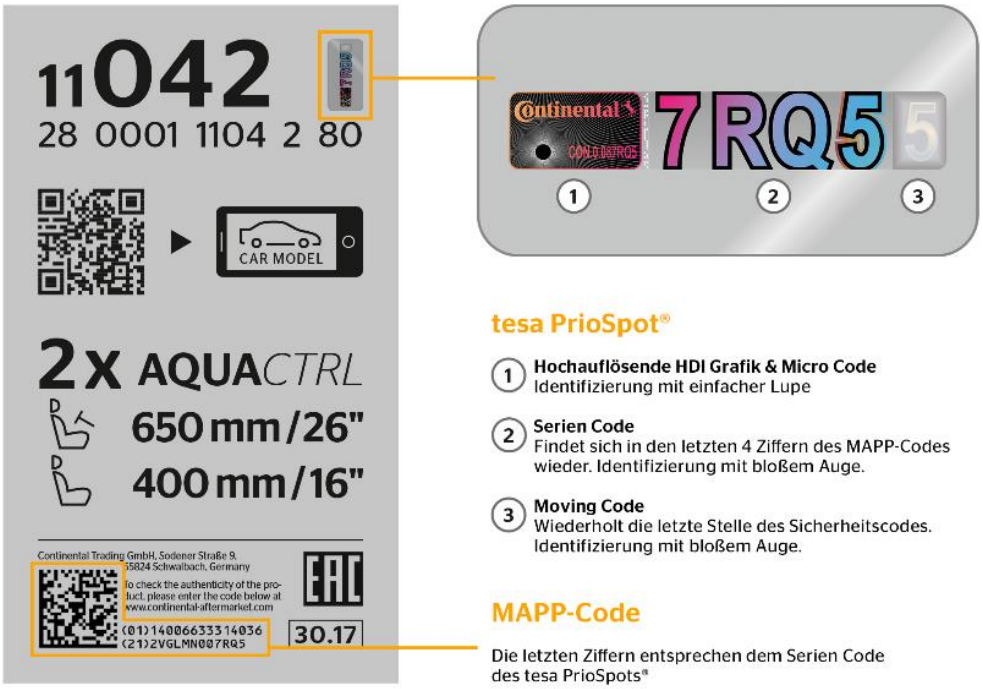


Figure 46

Figure 47

2.3.2.3 ZF Friedrichshafen

ZF Friedrichshafen AG, commonly referred to as ZF Group or ZF, stands as a global technological powerhouse, catering to a wide spectrum of industries, encompassing passenger cars, commercial vehicles, and industrial

technology. Nestled in Friedrichshafen, situated in the southwest region of Germany, this company is at the forefront of engineering excellence. Its fame largely emanates from its prowess in design, research and development, and the meticulous manufacturing of components, making it a titan in the automotive sector and ranking among the world's largest automotive suppliers. The scope of ZF's product offerings encompasses driveline and chassis technology meticulously crafted for both passenger cars and commercial vehicles. Beyond this, ZF extends its expertise to include specialized plant equipment, serving the needs of industries like construction equipment. However, ZF's influence doesn't cease with land-based vehicles; it transcends to a multitude of other domains, from the realms of rail transport to marine endeavours, aviation innovations, and even contributions to the defence sector. With a sprawling presence worldwide, ZF boasts a network comprising 168 production locations dispersed across 32 countries, and its global workforce, as of 2022, stands at an impressive figure, nearing 165,000 dedicated professionals.

Notably, ZF has not only excelled in the realm of product manufacturing but has also meticulously established an aftermarket service to cater to the needs of its discerning customers. To further enhance customer confidence and ensure the authenticity of its products, ZF has thoughtfully incorporated QR Codes on their product packaging. This ingenious feature empowers customers to perform an "Authenticity Check," assuring them of the genuineness of their purchase. In cases where customers encounter counterfeit or aftermarket concerns, ZF extends a proactive invitation to reach out to their dedicated division, ensuring that all customer queries and issues receive the attention and resolution they deserve.

2.3.2.4 Valeo

Valeo, a prominent global automotive supplier with its headquarters in France, plays a pivotal role in providing a diverse range of products to both automakers and the aftermarket. Operating in 33 countries worldwide, the Group boasts a workforce of 113,600 individuals and an extensive infrastructure that encompasses 186 production plants, 59 research and development centers, and 15 distribution platforms. The company's strategic approach revolves around a commitment to innovation and development, with a keen focus on high-growth potential regions and emerging markets. Adopted in 1980, the name Valeo, signifying "I am well" in Latin, encapsulates the company's dedication to well-being. Structured into four business units, Valeo's areas of expertise include:

1. Comfort & Driving Assistance Systems: Specialized in technologies aimed at enhancing driving safety, intuitiveness, autonomy, and connectivity.
2. Powertrain Systems: Devoted to developing innovative solutions for reducing CO_2 emissions through advancements in electrification, automated transmissions, and environmentally friendly engines for vehicles.
3. Thermal Systems: Focused on optimizing vehicle thermal management and ensuring passenger well-being.
4. Visibility Systems: Engaged in the development of technologies that guarantee optimal visibility and safety for drivers across various weather conditions.

Its Valeo Service activity is the entity responsible to supply spare parts to OEMs, customer, and aftermarket. Valeo is undergoing a comprehensive redesign of its product packaging to combat the prevalence of

counterfeit products. The new graphic design, named "Green Waves," features brand logos printed in varying sizes arranged in bands on cardboard. These bands are interspersed with the website address "valeoservice.com," which is also undergoing a redesign to align with the visual identity of the boxes. Regardless of the viewing angle, the packaging ensures easy readability of the brand name and website address. The printing is tailored to the box's size, with larger boxes having text bands four times larger than those on smaller boxes. While maintaining the brand's characteristic bright green colour, which is intrinsic to its DNA, a portion of products (estimated at 10-20% within Valeo) will continue to use the classic grey cartons. There will be present two color for packaging on market since the operation of entering this new measure will be gradually. The new packaging started in 2021 and was developed for B2B (business to business).

Valeo also uses various label to protect their product from being replicated, an example is the figure below which illustrate a compressor label where we could find the part number, serial number, the compressor type (size of model), and a unique identifying code.

Figure 48

2.3.3 Supplier/Engine Manufacturer

2.3.3.1 Mahle Multinational

MAHLE GmbH, a German automotive parts manufacturer headquartered in Stuttgart, stands as one of the world's largest automotive suppliers. Renowned for producing components and systems for combustion engines and their peripherals, MAHLE ranks among the top three global systems suppliers for engine systems, filtration, electrics, mechatronics, and thermal management. With a workforce of approximately 72,000 employees as of 2022, the company operates in 152 production plants and 12 major research and development centres across Germany, Great Britain, the United States, Brazil, Japan, China, India, Poland, Spain, and Slovenia. A dedicated team of over 6,000 development engineers and technicians collaborates globally to pioneer new products and systems for MAHLE's clientele.

The roots of MAHLE trace back to 1920 when engineer and pilot Hellmuth Hirth, alongside others, established a small workshop in Cannstatt. This workshop, initially focused on developing a two-stroke engine, witnessed the entry of Hermann Mahle as the company's seventh employee on December 1, 1920—a significant date

now recognized as the birth of the present-day Mahle Group. Recognizing the need for diversification beyond engine testing, the company embarked on a venture into piston production. While traditional pistons were made of cast iron, Mahle's innovative spirit led them to experiment with lightweight alloy pistons for combustion engines.

Mahle Powertrain Ltd, the wholly owned engineering services division of Mahle GmbH, operates with its headquarters in Northampton, UK, and a sister company in Plymouth, Michigan, USA. Specializing in the design, development, and testing of internal combustion engines, Mahle Powertrain provides an extensive range of engineering services to its global customer base.

Mahle is very active to counteract against counterfeited products. On their site, under “Brand Protection”, there are several instructions, suggestions, warnings to detect fake parts and understand the solutions implemented by the company. The company has adopted few solutions, developed internally, and it uses a third company to offer even better protection.

oneIDentity+ is a manufacturer-independent service platform to support role-specific mobile processes. It allows the tracking of products, the display of product, marketing, and maintenance information, the connection to customer loyalty systems. All participating manufacturers mark their products with a unique GS1 accordant data matrix code that could be checked on the platform. By using the oneIDentity+ app the customer and all those involved in the value chain can scan this code and gain access to target-group-specific information and value-added services worldwide, 24 hours per day.

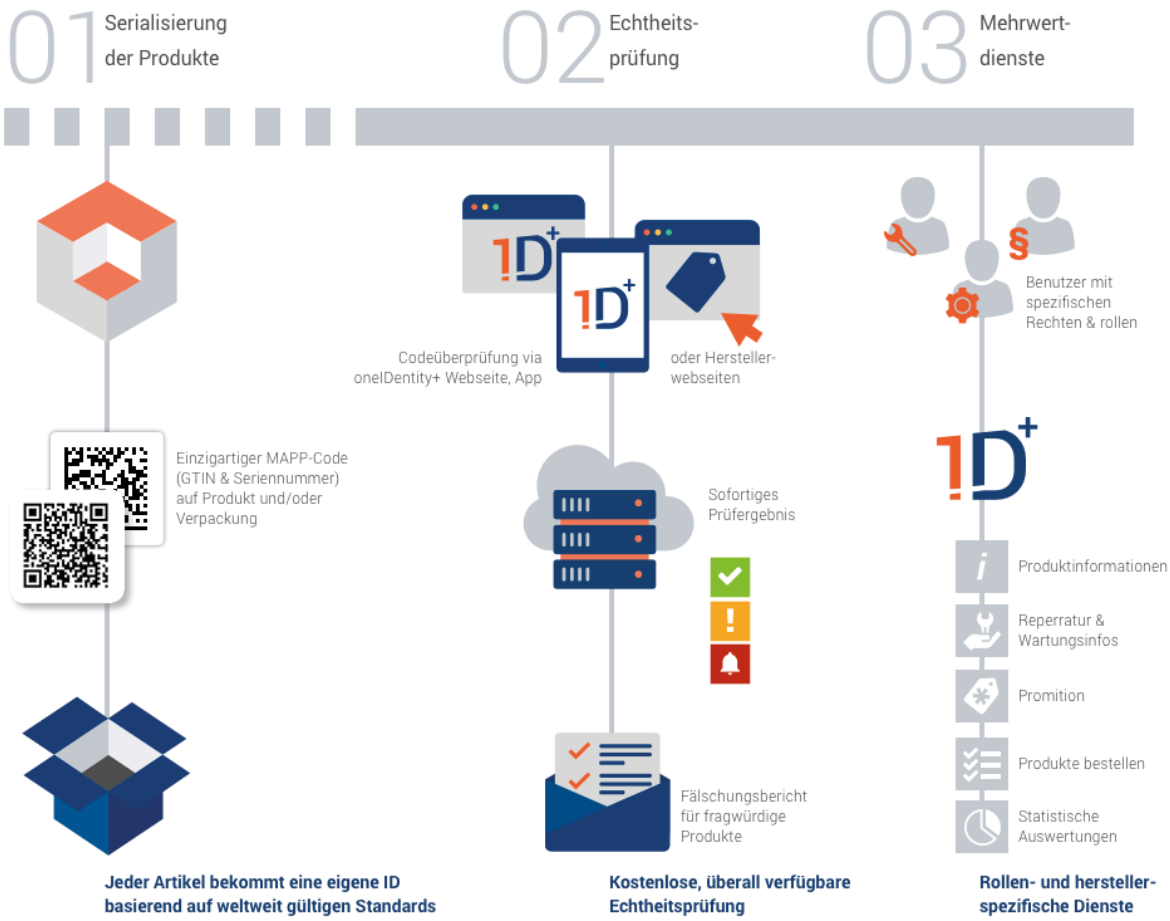


Figure 49

The company opted for a simple and clear packaging for its products. Bold colors, concise information, and clear design also ensure easy handling and fast identification in the warehouse. This design enables to have only essential information and all relevant details immediately, reader- friendly position of product description.

Mahle recently renewed its label. The process started on December 2016 and should be now complete, but I will also report the old label. The old one presented a special label that allowed customer to check the authenticity offline by using these four key points:

1. HDI star for high-resolution copy protection.
2. Mahle logo in shimmering rainbow colors (most easily visible when is held up to a direct, artificial light source).

3. LensCode, the last 2 digits of the random code, became visible with the special filter.
4. Serial number (black, outlined in shimmering rainbow colors) that corresponds to the last 6 digits of the random code.

Figure 50

The new label will present a 12 digits barcode, named universal product code (UPC), to allow a product to be uniquely identified by manufacturer and product classification. The customer can scan the QR code and immediately see the result; GREEN means that the products is a genuine or original part; YELLOW means that maximum number of checks for this code have been exceeded and so could be a fake; RED there are errors that do not match with the principle adopted to create a code. Another label called the security strip which is used to shown that the package has not been opened. Once it is removed the word “OPEN” became visible.

Figure 51

Figure 52

2.3.3.2 Tenneco

Tenneco, previously known as Tenneco Automotive and originally named Tennessee Gas Transmission Company, operates as an original manufacturer of automotive components, specializing in aftermarket ride control and emissions products. The company's headquarters are situated in Northville, Michigan, United States. A significant development occurred on October 1, 2018, when Tenneco successfully concluded its acquisition of Federal-Mogul Corporation. Subsequently, in February 2019, Tenneco unveiled plans to separate its automotive aftermarket suspension components, forming the distinct entity known as DRiV Incorporated.

It was acquired in February 2022 by Apollo Global Management for an amount of $7.1 billion.

2.2.3.2.1 Federal-Mogul Corporation

Federal-Mogul Corporation stands as an American entity dedicated to the development, manufacturing, and supply of products spanning automotive, commercial, aerospace, marine, rail, off-road vehicles, and applications in industrial, agricultural, and power generation. Established in 1899 in Detroit by J. Howard Muzzy and Edward F. Lyon under the name Muzzy-Lyon Company, they initially focused on producing mill supplies and rubber goods. Concurrently, they introduced a subsidiary, the Mogul Metal Company, pioneering innovations in various bearings. Notably, the company utilized its proprietary Babbitt metal alloy called "Mogul," trademarked as "Mogul" and "Duro." In 1924, the merger of Muzzy-Lyon and Federal Bearings and Bushing resulted in the formation of the Federal-Mogul Corporation.

Operating with two distinct business divisions, namely Federal-Mogul Powertrain and Federal-Mogul Motorparts, the Powertrain division specializes in the design and manufacturing of original equipment powertrain components and system protection products. This division's diverse product line encompasses powdered metal parts, space suits, and a comprehensive range of items such as engine bearings, pistons, piston pins, piston rings, cylinder liners, valve seats and guides, spark plugs, ignition coils, transmission products, technical textiles, and connecting rods. The corporation has a notable presence both in the United States and internationally.

Federal-Mogul provides three security layers to enhance their security. The first layer is the permanent self-adhesive a label used to show that the package has not been opened before. Special label design means any attempt to remove or swap the label will resulting in tearing.

Figure 53

The second layer is the PrioSpot® label, also used by AG Continental. This code is different for each package and contains the last 4 digits of the Alphanumerical Code. The code and the DRiV (Federal-Mogul) logo shimmer in the rainbow colors, only when face direct light. The last letter will be different for every label and is visible only to direct light illumination. In addition, this digit will move up or down when the customer change the angle of the PrioSpot®.

Figure 54

The third layer is the verification of the Alphanumerical code and the Data matrix present on every label, see figure above to see its location. The customer or the retailer could verify the code by entering it manually on the site (under the voice Support-Anti-Counterfeit) or scanning the data matrix with a 2D scanner device or a mobile phone.

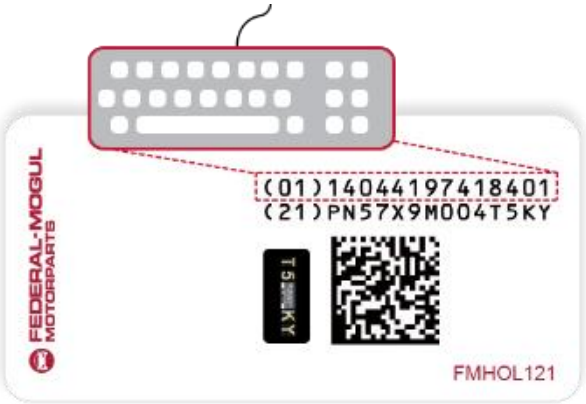


Figure 55

Figure 56

Figure 57

2.3.4 Special Mention

Within this dedicated section, aptly named "Special Mention," we spotlight an exemplary instance featuring an automotive manufacturer. It's essential to clarify that companies of this nature should not be perceived as direct competitors. This distinction arises from the distinct customer segments that these companies cater to. The purpose behind referencing them is to glean insights from the solutions they have implemented. This automotive manufacturer is merely used as an illustrative example, shedding light on the wealth of readily available information accessible through their website.

2.3.4.1 FORD

Based in Dearborn, Michigan, the Ford Motor Company stands as an American multinational automobile manufacturer with a rich history. Established on June 16, 1903, by the visionary Henry Ford, the company became synonymous with pioneering manufacturing methods that revolutionized the automotive industry. Ford's innovative approach included the implementation of large-scale manufacturing for cars and the efficient management of industrial workforces. Notably, the introduction of moving assembly lines and intricately engineered manufacturing sequences marked a turning point, and by 1914, these groundbreaking methods had gained global recognition under the term "Fordism."

How to check for counterfeit parts:

- Serial number and Hologram: All genuine spare parts come with specific serial numbers. Also find the specific hologram of the manufacturer as it cannot be counterfeited.
- QR Code: Most spare parts come with a QR code that can be scanned using a smartphone to ensure that the part is genuine.
- RFID Tags: Genuine parts come with RFID tags which can be traced by the manufacturer.
- Packaging: Carefully inspect the packaging. Counterfeit parts come in cheap packaging.
- Instructions: Check if instructions are incomplete or incorrect. Check for misspellings.

Or by giving these instructions to their supplier which must be insert them on the spare parts:

- Ford Oval Trademark
- Global Supplier Database Code
- Ford Long Part Number

These measures will help Ford to keep track of their product along the supply chain.

3. Development of a Comparison Process

In this chapter, I'll clarify how I created the Excel document. This document serves as a practical example, a sort of “use case”, aiming to connect the engine parts produced by the company with the previously discussed anti-counterfeiting solutions. Consider this use case as an initial step in understanding this connection. The company has the option to expand on it by adding more relevant information that I couldn't share externally.

To illustrate this use case, I utilized several tables, including a final table or matrix. I chose this straightforward method to generate results that are easily understandable for the company, aiding them in comprehending the construction of the table.

The Excel document has two pages: one is labelled "Anti-counterfeiting Solutions," and the other is named "Engine Components". In the first page, there is a table in which I listed all the devices discussed in the initial chapter and evaluated them objectively using different parameters. The second page follows a similar structure. On the left side, there is a table listing engine parts with assigned importance weights for the same parameters used on the first page. The right side features a matrix connecting spare parts to different solutions.

The Table 1 illustrate the values used to give a weight to the different parameters.

Low	1--2
Medium	2--3
High	3--4
Very High	5

Table 1

For this use case have been selected four parameters that were the most suitable to analyse the various solutions and the spare parts with the information available. The indicators are:

- Cost.
- Complexity.
- Reliability (Security).
- Information quantity stored.

The mental process used to assign solutions and spare parts to these attributes is explained below. In the first page, they are employed to rank different devices, while in the second, they are analysed to reflect the needs of the company.

On the first page, there is a table that contains all the anti-counterfeiting solutions listed in the first chapter. The weight given to these parameters was based on the information reported in the first chapter and on some assumptions, which are clarified in the Table 2.

Complexity refers to how a solution operates and how challenging it is to put that solution into action. I've also thought about the fact that some solutions require additional devices to function; for instance, RFID needs a second device to read the information. Therefore, I considered how straightforward or intricate these interactions might be. I found machine interactions to be the easiest, while those involving human staff were more complicated. An example of how complexity has been examined is the following one:

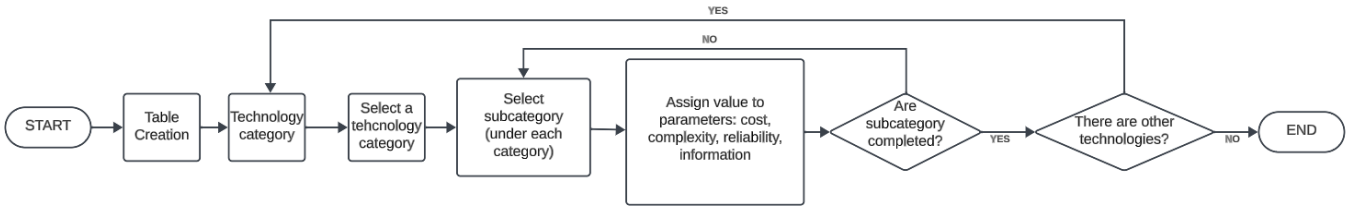
“Implementing a QR Code is very straightforward, and understanding how it works is easy. On the other hand, implementing Security Holograms requires a precise process, and its functioning is more complex than that of a QR Code. A QR Code interacts with a smartphone or a reader device in a simple way, whereas the interaction between holograms and an inspector is quite intricate. The supervisor needs to know exactly what to look for.”

To grasp my thought process in assigning weights, let's consider the parameter "Reliability." I ranked them from least secure to most secure, assigning the highest value to the most protective solution. Following this logic, I gave a score of 1 to the QR Code and 5 to the Blockchain, as the latter is expected to be the most secure option.

Parameters	Mental Process	1--2	2--3	3--4	5
Cost	How much cost?	Low	Medium	High	Very High
Complexity	How solutions works/interacts?	Easy/Machine	Medium/People, Machine	High/ People	Very High/ People, Machine
Reliability	Level of security?	Low	Medium	High	Very High
Information quantity stored	How much information it contains?	Few	Limited	High	Endless

Table 2

On the first page, the green boxes show devices commonly used on paper or in other applications, I also added a few words next to them to explain how they could be used. I didn't include these boxes on the second page to keep the document concise and easier to read. While creating that page, I decided to keep the same classification used in the index and the first chapter to clearly represent the different classes.



Graph 1

On the second page, I worked closely with the company to list several parts used in manufacturing an engine. I identified these components by accessing the company's databases. Initially, the extraction yielded 450-500 spare parts from an engine. To streamline the list, I collaborated with colleagues and made some assumptions to reduce it. This reduction was necessary because some parts would be unnecessary (for examples a screw that cost few cents does not need to be protected) for the company, and we aimed to create a matrix that would be easy to read and understand.

In our first attempt, we used the specific cost of each component to highlight the most expensive ones, thinking they were the most important to protect due to their high cost. However, upon reviewing the list, we realized that some high-cost parts had a long useful life and didn't need protection. We understood that

high cost was not a reliable indicator, as some expensive parts are rarely sold as spare parts. If a part will not be sold after, it will have not sense to develop or include security features against counterfeiters. After considering this, we decided to use an internal code that explains or identifies the useful life of the parts. This helped us narrow down the list to 33 components that are most commonly acquired in the aftermarket or as spare parts after the engine is sold. These 33 spare parts have a relatively short useful life compared to others. The main assumption was: “If a component has a short life, it means that it will be re-acquired in the future. So, it is important for the company to protect this part or the customer once they will have to replace it”.

On the left side of the second page, I made a table which contains the weight given to each component for all the attributes considered. Even though cost was rejected as a classification criterion, I used the "Monetary Value" column (based on specific cost) to estimate the weight of each parameter. Table 3 summarizes the methods used to rank these variables.

For the Cost column, I assumed that parts with a higher Monetary Value are those the company wishes to protect more or is willing to spend more money on to implement anti-counterfeiting solutions.

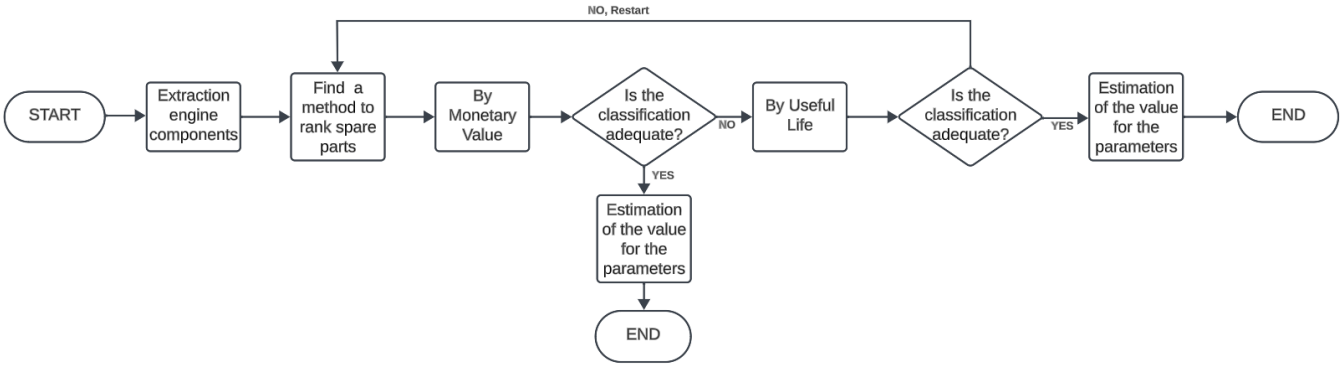
Regarding the Reliability column, I assigned a similar value as for the Cost column. The idea was that if a part is crucial enough for the company to protect, even at a higher cost, security must be a significant factor in combating counterfeiters.

Complexity was considered in terms of the possibility to install a particular solution directly on the analysed parts. I examined the drawings of each piece, estimating whether there was enough free space. Following this principle, a screw, for example, would have a value of 5 because applying any solutions to it would be impossible due to its small size and shape.

The "Information Quantity Stored" column was challenging to establish due to the nature of the information that the company chooses or must provide. I assumed that spare parts with high cost and high security needs could involve more information due to their importance and complexity.

Parameters	Mental Process	Weight (1,2,3,4,5)
Cost	Based on Monetary Value	Higher mon. value, higher weight
Complexity	Based on the drawing/size	Lot of space, high value
Reliability	Based on Monetary Value	High cost, high weight
Information quantity stored	Based on Cost and Security	Assumed

Table 3

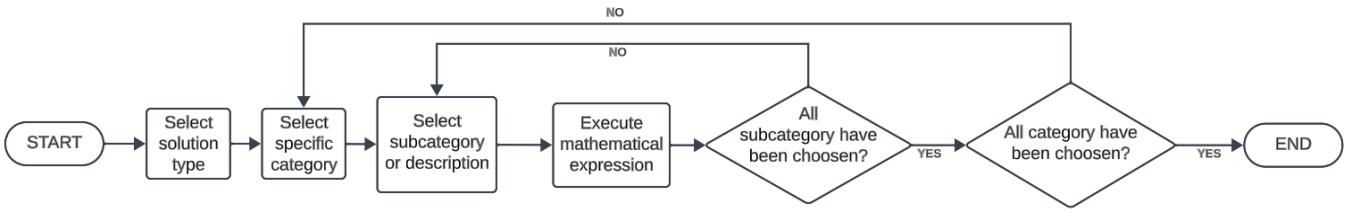


Graph 2

Then on the right side of the page, I developed the matrix used to link the various solutions with the spare parts. Between the table containing engine parts and the matrix, there's a column with barred cells to keep them separate.

The matrix follows a specific structure, with the left column listing the different engine parts, which is the same as the first column (Column A) on the page. I rewrote it to avoid confusion when looking for a specific value for an engine part.

In the first row of the matrix (row 2 of the Excel paper), various anti-counterfeiting devices are listed, using a classification similar to the one in the first paper. The yellow boxes represent a broader category of solutions, including all the devices in the cells next to it until a new yellow box is reached. Due to space constraints, I wrote above different cells belonging to the same family the name of the family.



Graph 3

The matrix was created using a mathematical expression based on weighted sums. The expression involves multiplying values within the same "Parameter" column for a solution and an engine part. The final values are obtained by summing all the previous values obtained for each parameter.

Table 4 illustrates the second page for two engine parts and some anti-counterfeiting solutions. We can see that the first six columns represent the Engine part table, while the other are the matrix. In the matrix we

could see a yellow box and some “family name” above some solutions. The first value, 14, represents the value that the RFID passive has when linked to High Pressure Pump.

		Parameter 1	Parameter 2	Parameter 3	Parameter 4			Solutions	RFID	RFID	RFID
Description	Monetary Value	Cost	Complexity	Reliability	Information quantinty stored		Description	ELECTRONIC	Passive	Active	BAC
HIGH PRESSURE PUMP	Very High	5	1	5	3		HIGH PRESSURE PUMP		14	25	20
TURBOCHARGER	Very High	5	2	5	3		TURBOCHARGER		15	26	21

Table 4

The table is meant to be read row by row to determine the best solution for each engine component. The highest value in a row indicates the optimal result, representing the most effective anti-counterfeiting devices to be implemented on that specific spare part. When assigning weights for each parameter in the engine table, I prioritized Cost and Security as the most important factors. Since the highest value (5) signifies the utmost importance for the company, the best solution is identified by the greatest sum of weights.

The company can then choose to adopt the absolute best solutions by examining all the values in a row. Alternatively, it may decide among the best solutions within a specific class or family.

Blockchain is a unique technology with versatile applications, such as tracking a product's journey from production to sales throughout the supply chain or facilitating payments. The values in the Blockchain column are the highest values in each row, as my research indicates that blockchain is considered the most comprehensive device for product protection. Based on this information, I assigned a value of 5 to each parameter, but the company should consider additional factors or attributes when deciding whether to implement it or not. Blockchain is a unique technology with versatile applications, such as tracking a product's journey from production to sales throughout the supply chain or facilitating payments. However, evaluating its effectiveness in this document was challenging because it largely depends on the company's goals and the capabilities of the team responsible for implementing and developing the blockchain code.

In summary, the use case serves as an initial step to identify the best solutions for individual spare parts. The potential revenue and reputation losses associated with counterfeit goods should motivate FPT Industrial to invest the necessary resources in minimizing this problem. The company's next move should involve gathering more information about current technologies, including studying competitors.

To optimize this use case, expanding the considered parameters is crucial. This entails creating a comprehensive list that includes all possible variations and addresses the specific needs of the company. For instance, considering the attribute "Cost", the attribute in the first page, represents how much it would cost to the company to purchase that anti-counterfeiting solutions. FPT Industrial should also weigh the option of developing these solutions internally, leading to a decision of whether to make or buy. By broadening the scope of attributes considered, the company can provide a more detailed description of the solutions and better understand their connection with engine parts.

Another improvement to the use case involves aligning company strategies with its needs. This alignment can help avoid unnecessary operations for less critical pieces and provide a more accurate evaluation of certain parameters.

The excel document do not take into consideration the combination of more technologies together such as a label with a hologram and/or a QR Code printed on it. Combining these devices could impact certain properties in positive or negative ways, enhancing the parameters in the use case. For instance, combining two affordable technologies might provide better security features than a third option that is more expensive.

To take advantage of the opportunities that may arise from these combinations, the company should first assess each technology individually. Once they have acquired the necessary knowledge during this initial step, they can then proceed to conduct several trials to determine if there are any beneficial combinations.

4. Conclusion

There are numerous anti-counterfeiting solutions available for this sector, each with its own pros and cons. The market of counterfeits goods its forecasted to grown due to a general growth of the of the environment. As seen in chapter two Ecommerce and aftermarket sales are expected to grow and to generate more revenue, this could represent a chance for counterfeiters. This growth presents an opportunity for counterfeiters. The current economic situation, conflicts, and inflation may further boost the demand for counterfeit products as consumers look to save money and accept riskier parts. Companies specializing in security devices and those producing protective packaging are expanding their market presence. The projected demand for these companies is on the rise, with an estimated Compound Annual Growth Rate (CAGR) of 12.6% between 2022-2029, indicating a growing interest in solutions to combat counterfeiting.

Analysing competitors provides insights into how these companies are developing security features and underscores the severity of the problem. FPT Industrial should carefully examine these companies to potentially adopt the best solutions and enhance the safety of their products and customer communication. Some competitors have dedicated webpages on "brand protection" or counterfeit parts, explaining the differences between genuine and fake components. Certain solutions even include a page where customers can check the authenticity of purchased parts using a numerical code to detect if the part is genuine, show sign of possible tampering, or counterfeited. FPT Industrial should consider creating webpages and articles to explain their solutions, guide customers on how to interpret and understand them, and provide a means to check authenticity. It's crucial to ensure these pages are easily accessible on their website, since finding them with the most obvious key words was challenging for some competitors.

In conclusion, there isn't a one-size-fits-all solution. Each product has different technologies that can enhance its protection. Therefore, FPT should be able to capitalize on this variety and choose the best solution for each individual spare part. Additionally, they need to decide on the best overall strategy, considering aspects like communication, marketing, and whether to make or buy the protection. FPT Industrial should also think

about combining different technologies, like using a label with a QR code. By studying these solutions individually or together, the company can exploit all the potential advantages.

SITOGRAFIA:

https://www.thespiritsbusiness.com/2023/04/how-the-industry-is-tackling-fake-alcohol/

https://uibm.mise.gov.it/index.php/it/lotta-alla-contraffazione/servizi-per-imprese-e-consumatori/tecnologie-anticontraffazione/sot-servizio-orientamento-tecnologie-anticontraffazione/overview-tecnologie-anti-contraffazione

https://www.ologrammi.com/

https://www.europeanpharmaceuticalreview.com/article/170913/the-latest-on-pharmaceutical-counterfeiting/

https://www.uspharmacist.com/article/counterfeit-meds

https://www.vericode.it/it/anticontraffazione-le-migliori-tecnologie-di-protezione

https://temera.it/it/news/blog/smart-health-e-tracciabilita-nella-filiera-del-farmaco.html

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4001489/

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9031510/

https://collectid.io/what-is-the-best-anti-counterfeit-technology-in-2023/#:~:text=Automotive%3A%20Companies%20in%20the%20automotive,protect%20their%20products%20from%20counterfeiting

https://www.sanita24.ilsole24ore.com/art/europa-e-mondo/2019-02-08/farmaci-operativo-domani-passaporto-elettronico-ue-anti-contraffazione-il-bollino-italiano-deroga-fino-2025-125408.php?uuid=AF1MDtK&refresh_ce=1

https://www.digital4.biz/executive/contraffazione-alimentare-guida-alla-tutela-dei-prodotti-e-dei-consumatori/

https://www.thespiritsbusiness.com/2023/04/how-the-industry-is-tackling-fake-alcohol/

https://www.pmi.com/markets/italy/it/sostenibilita/sostenibilita-sociale/lotta-all'illecito

https://www.ilsole24ore.com/art/il-falso-made-italy-tavola-ora-vale-120-miliardi-euro-AEQjRbfB

Politecnico di Torino

https://www.ilsole24ore.com/art/contrabbando-sigarette-fumo-10-miliardi-imposte-ue-AEVJrYfE

https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2022/07/11/Report-05-Il-mercato-illecito.pdf

https://www.bancaditalia.it/compiti/emissione-euro/contraffazione/index.html?dotcache=refresh

https://en.wikipedia.org/wiki/Central_Bank_Counterfeit_Deterrence_Group#External_links

https://www.ecb.europa.eu/euro/banknotes/current/security/html/index.it.html#feel

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32014L0040

https://www.adm.gov.it/portale/sistema-europeo-tracciamento-prodotti-tabacco

https://www.adm.gov.it/portale/documents/20182/1106814/Encoding+of+Unique+Identifiers.pdf/214b6dea-3776-4778-a1ec-f1bce57cb632

https://www.carabinieri.it/in-vostro-aiuto/consigli/banconote-e-monete-false

https://eur-lex.europa.eu/eli/reg/2011/1169/2018-01-01

https://collectid.io/what-is-the-best-anti-counterfeit-technology-in-2023/

https://food.ec.europa.eu/safety/labelling-and-nutrition/food-information-consumers-legislation_en

https://collectid.io/what-is-the-best-anti-counterfeit-technology-in-2023/

https://www.investopedia.com/terms/o/oem.asp#:~:text=OEM%20vs.-,Aftermarket,been%20sold%20to%20a%20consumer

https://en.wikipedia.org/wiki/Automotive_aftermarket#References

https://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement

https://ustr.gov/acta

https://www.grandviewresearch.com/industry-analysis/aftermarket-automotive-parts-market#:~:text=Report%20Overview,to%20Grand%20View%20Research%2C%20Inc

Politecnico di Torino

https://www.alliedmarketresearch.com/automotive-aftermarket-market-A17049

https://www.fortunebusinessinsights.com/automotive-after-market-102613

https://straitsresearch.com/report/automotive-after-market

https://uibm.mise.gov.it/images/SA2021/Rapporto2021.pdf

https://www.fleetowner.com/equipment/article/21267873/genuine-vs-counterfeit-truck-parts

https://www.worldtrademarkreview.com/global-guide/anti-counterfeiting-and-online-brand-enforcement/2019/article/counterfeit-automotive-parts-increasingly-putting-consumer-safety-risk

https://authena.io/it/automotive-aircraft-spare-parts-counterfeiting/

https://www.redpoints.com/blog/fake-car-parts/

https://www.maximizemarketresearch.com/market-report/global-anti-counterfeit-automobile-packaging-market/99147/

https://ennoventure.com/blogs/automotive-vehicle-fake-spare-parts-anti-counterfeiting/

https://hedgescompany.com/blog/2021/11/auto-parts-ecommerce-38-billion-in-2022/

https://www.a2c2.com/

https://www.worldtrademarkreview.com/global-guide/anti-counterfeiting-and-online-brand-enforcement/2021/article/counterfeiting-and-piracy-in-2021-the-global-impact

https://www.fordbrandprotection.com/

https://www.me.ford.com/en/jor/ownersite/counterfeit-parts/

https://ihma.org/holograms-drive-diesel-engine-aftermarket-parts-authentication/

https://www.cumminsdksh.com/th/cummins-anti-counterfeit/

https://en.wikipedia.org/wiki/Cummins

https://ihma.org/holograms-drive-diesel-engine-aftermarket-parts-authentication/

Politecnico di Torino

https://www.perkins.com/en_GB/aftermarket/maintenance/genuine-experience/genuine-parts-hologram.html

https://en.wikipedia.org/wiki/Perkins_Engines

https://spare.avspart.com/caterpillar/shaft/3043269/

https://en.wikipedia.org/wiki/Caterpillar_Inc.#

https://parts.cat.com/en/catcorp/231-8137?_gl=1*gmjm57*_ga*MjczMDcwMTgxLjE2OTY2MDE5MTI.*_ga_RJ3G1WBXL7*MTY5Njg1NTY3NC4yLjEuMTY5Njg1NTcyMy4xMS4wLjA.

https://www.bosch.com/stories/from-research-to-a-commercial-aiot-product-secure-product-fingerprint/

https://www.boschaftermarket.com/xc/en/keysecure

https://isuzu-malawi.com/parts/fake-parts/

https://www.content.isuzu.com.au/news-articles/imitation-without-flattery-the-consequences-of-buying-counterfeit-parts/

https://www.isuzu-intl.com/parts/

https://biasharaleo.co.ke/isuzu-east-africa-takes-the-fight-against-counterfeit-goods-head-on/

https://www.continental-aftermarket.com/en-en/products/spare-partsrepair-parts/filters/oil-filters

https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Anti_Counterfeiting_Technology_Guide/2021_Anti_Counterfeiting_Technology_Guide_en.pdf

https://it.wikipedia.org/wiki/Continental_AG

https://www.continental-aftermarket.com/en-en/services/product-and-brand-protection/continental-brand-protection

Politecnico di Torino

https://www.tesa.com/en/industry/automotive/supplier-systems/powertrainhttps://it.wikipedia.org/wiki/ZF_Friedrichshafen

https://aftermarket.zf.com/en/aftermarket-portal/services-and-support/faq/amp_uni_ps_faq.jsp

https://en.wikipedia.org/wiki/Weichai_Group

https://en.weichai.com/cpyfw/wmdyw/hfwsc/yp/tjcp/201907/t20190711_53091.htm

https://en.wikipedia.org/wiki/Valeo

https://valeo.prowly.com/136665-valeos-new-product-packaging-modern-and-practical

http://www.valeocompressors.com/en/faq

https://en.wikipedia.org/wiki/Mahle_GmbH

https://en.wikipedia.org/wiki/MAHLE_Powertrain

https://www.mahle-aftermarket.com/eu/en/brand-protection/

https://en.wikipedia.org/wiki/Federal-Mogul

https://www.drivparts.com/it-it/support/anti-counterfeit.html

https://www.drivparts.com/en-gb/support/anti-counterfeit.html

https://www.drivparts.com/en-eu/support.html

https://www.drivparts.com/en-ae/support.html

https://www.aftermarketnews.com/federal-mogul-motorparts-introduces-advanced-brand-protection-features-fp-diesel-products/

https://en.wikipedia.org/wiki/Tenneco

https://www.adm.gov.it/portale/documents/20182/1106814/Encoding+of+Unique+Identifiers.pdf/214b6dea-3776-4778-a1ec-f1bce57cb632