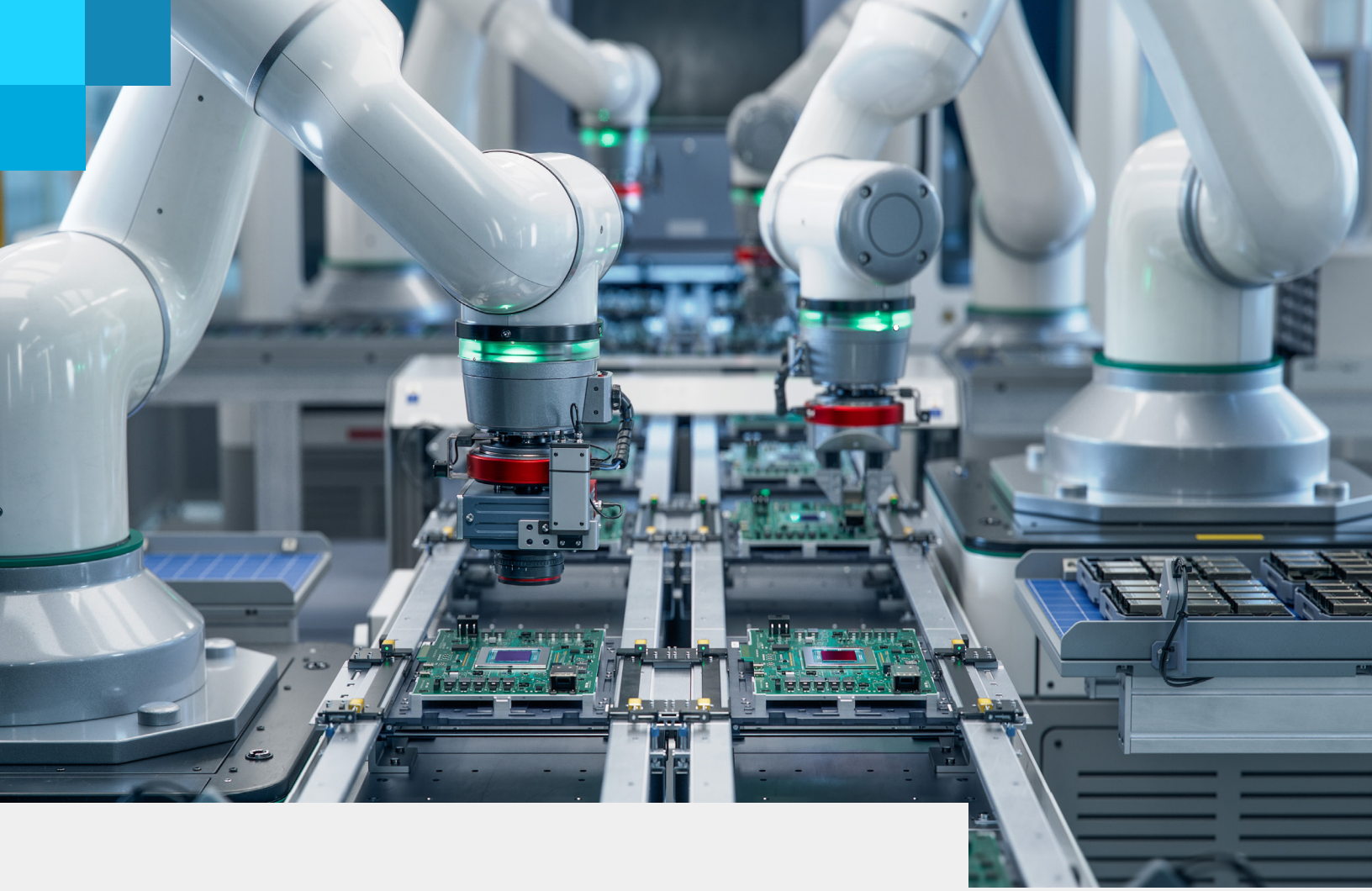
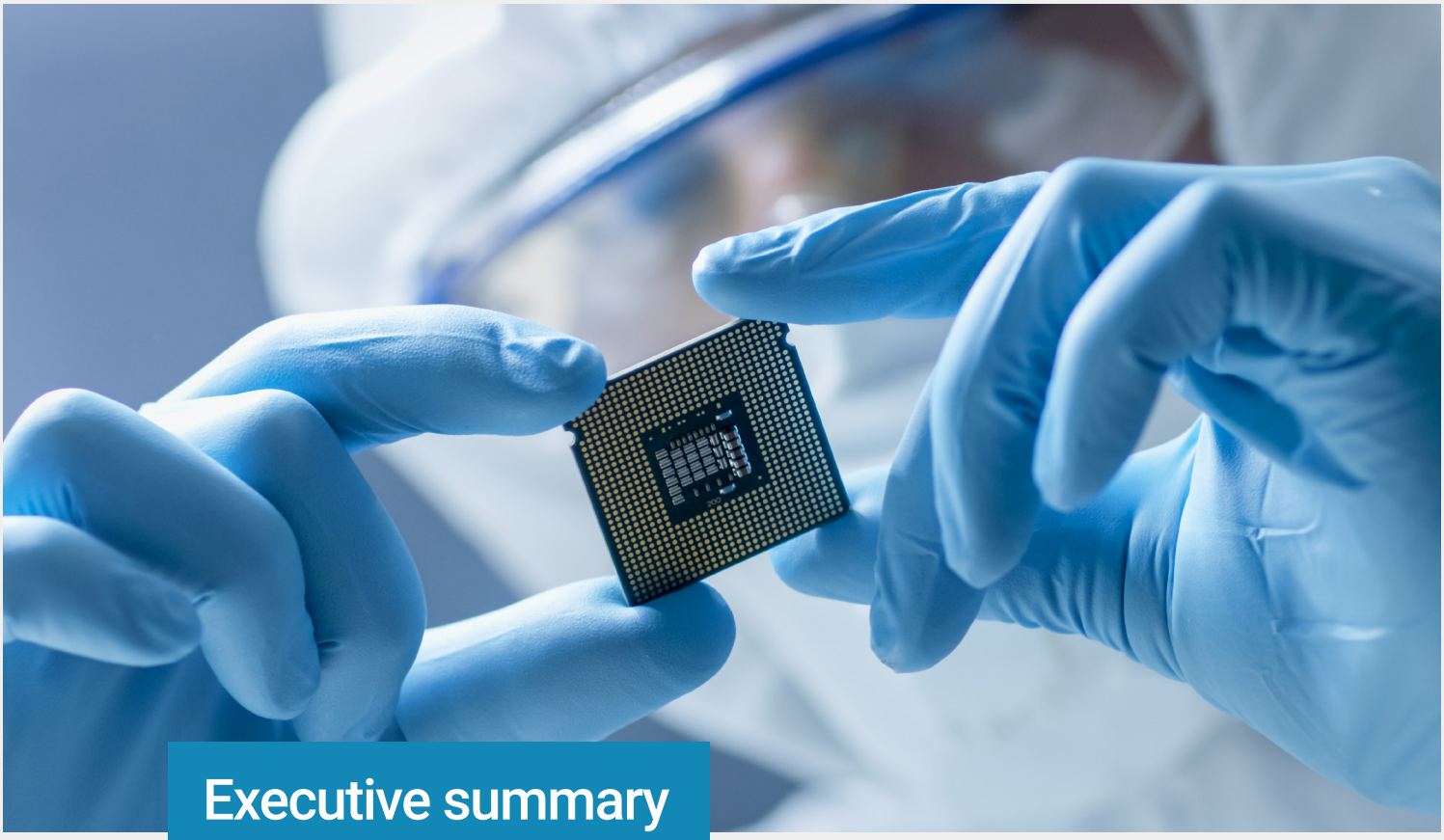


Counterfeiting: The rising threat to electronics manufacturers

A cloud-based labeling approach means better traceability, fewer labeling errors, and safer products

Loftware™

White Paper



Executive summary

As a serious challenge to today's global electronics supply chain, counterfeiting and grey market diversion of electronics components threaten the integrity of products for manufacturers. Counterfeits and obsolete electronics components create significant risks for manufacturers customers, and compromise health and safety for consumers. Clearly, new solutions are needed to improve electronics supply chain integrity and stability.

Unit item serialization is one of the most powerful anti-counterfeiting and anti-diversion measures available today. However, many manufacturers lack standardized and automated enterprise-wide labeling solutions as a foundation upon which serialization can be implemented efficiently and cost effectively. This is because many large electronics organizations, their suppliers, and their distributors still rely on a disconnected web of labeling processes and systems. Serialization technology cannot be applied consistently or affordably throughout a non-standardized labeling environment.

However, cloud-based labeling solutions can provide the first line of defense in today's complex high-tech electronics distribution environment. Cloud labeling offers a dynamic and data-driven approach for the creation of complex 1 and 2D barcode labels. It provides a platform for standardization, automation, scalability, and efficient maintenance, while allowing businesses to react quickly to evolving customer, regional and regulatory requirements, and ensures consistency across a global supply chain.

Cloud-based labeling solutions enable electronics manufacturers, suppliers, and vendors to meet performance and scalability requirements with power and flexibility. Then when a company is ready to add serialization technology, unique product identifier serial numbers can be integrated with minimal disruption and effort to provide a powerful deterrent to counterfeiting and diversion. Now is the time for all responsible electronics supply chain stakeholders to look to cloud solutions as the best rapid response strategy to such a critical supply chain challenge.

Counterfeits jeopardize lives and cost billions

Electronics counterfeits have been a hot topic for many years, however the magnitude and complexity of the challenges regarding counterfeit goods continue to grow as the counterfeiters become more advanced in their methods. For aerospace, military, and other high-tech industries, the discovery of counterfeits has ignited intense debate over how to lessen the alarming risks involved. Without a doubt, counterfeits or obsolete components can, sooner or later, fail to perform under critical circumstances. There are several factors which have contributed to the difficulty in understanding what to do about obsolete and counterfeit electronics, not least the lack of visibility of components as they travel through the supply chain.

Many experts insist that the high prevalence of electronic counterfeits has arisen as a by-product of the grey market, which is the unauthorized sale of new, branded products diverted from mainstream distribution channels. The grey market has spawned a fraudulent and unreliable distribution system based on a marketplace clamoring for price discounts and high availability for technology products. Counterfeits have crept into distribution networks through rogue component design houses fronting as manufacturers, which then sell those products to independent distributors. After distributors obtain these products illegally, components enter the grey market, are sold at sharp discounts over the Internet, and are often offered alongside genuine components making it difficult to know which products are authentic and which are not.

The “underground” supply chain also handles obsolete parts found in e-waste and used in remanufacturing. These obsolete parts have made their way into the hands of buyers who believe they are getting brand new products. In this way, counterfeit and obsolete electronics have been discovered in missile guidance systems and hundred-million-dollar aircraft, causing serious security problems for the U.S. Department of Defense and its contractors. Who made these counterfeits, and are they programmed with malicious software from terrorist organizations designed to divert flights, radars, or missile controls? What about tampering with commercial aircraft electronic components? What happens when an obsolete component fails? Worst case scenario, safety and even lives can be put at risk.

How are counterfeits identified?

What methods is the Electronics industry using to identify counterfeits? It's certainly not as easy as detecting a knock-off Louis Vuitton bag or a Rolex watch. A savvy consumer can often tell in a glance whether a designer handbag or a pair of shoes is genuine or not. But electronics counterfeits hide deep within products or systems and are not easy to detect. Inspectors cannot open every product to test components inside.

The most obvious way to avoid counterfeits is to buy parts exclusively from authorized OEMs (Original Equipment Manufacturers). The National Defense Authorization Act uses this approach under Section 818, stipulating that all contractors and sub-contractors doing business with DOD must purchase their parts from authorized OEMs. But OEMs may have unknowingly included obsolete or counterfeit parts in their manufacturing process.

Various technologies do offer partial solutions to the counterfeiting problem. Companies can scrutinize packages for signs that pins have been straightened or indications that labels have been sanded and repainted. They can also perform more detailed analysis using X-ray, scanning electron, or acoustic imaging to look inside a package for things that might be amiss, like the improper placement of a chip within its package. In addition, DNA, which adds forensic markers to products for the military, has been used on a limited basis.

Meanwhile, counterfeiters are getting better at their craft every day. They buy discarded components on the cheap and sell them at full retail price, then use those profits to get even better at hiding their components. Ethical distributors face competitive challenges since they buy and sell components at razor thin margins. Any testing just adds to their costs, and it is simply not practical for most companies that buy subsystems to test every component within them.

Now imagine a different scenario where your supplier remotely accesses and prints your labels. By leveraging data directly from your ERP and merging it with supplier actions, you ensure that inbound materials are labeled and formatted the right way — your way, securely. Receiving quickly scans and processing shipments without delay, eliminating the need to store so much additional supplier managed inventory. In addition, you can track goods with unprecedented visibility to respond faster and smarter to fluctuations in supply and demand.

Global companies need to be able to seamlessly provide their manufacturers and supply chain partners with instant access to their labeling solution. This will enable the company to ensure that parts and raw materials are all sourced from vetted suppliers, will ensure that upstream parts can be made available for downstream use, and will ensure rapid traceability in the event of a recall. A comprehensive cloud-based labeling solution can offer efficiencies to manage challenges associated with the rise of intermediate inputs, allowing manufacturers and distributors to manage supplies without relabeling, saving on time, materials, handling, and storage costs.

What about the commercial supply chain?

Counterfeiters view the commercial supply chain as an attractive route to get counterfeit goods to market. The commercial market is much larger and more diversified than the public sector supply chain, particularly in the area of defense, the level of testing is lower, and product life cycles are much shorter. This gives counterfeit parts more time to hide and counterfeiters more time to sell their wares. Global companies need to be able to seamlessly provide their manufacturers and supply chain partners with instant access to their labeling solution. Counterfeit parts have been found in servers, routers, storage hardware, and other electronics systems. These systems enable communications, transportation, power, and critical infrastructure to run our daily lives.

For example, here is a list of some of the electronic products under FDA jurisdiction:

- Television receivers
- Computer monitors
- X-ray machines (including medical, research, industrial, and educational)
- Electron microscopes
- Black light sources
- Welding equipment
- Alarm systems
- Microwave ovens (devices that generate microwave power)
- All lasers (including low power lasers such as DVD and CD readers/writers/players) and other light emitting devices (Infrared and Ultraviolet)
- Ultrasonic instrument cleaners
- Ultrasound machines
- Ranging and detection equipment, such as laser levels

Unfortunately, most solutions today only detect counterfeit components after they enter the supply chain, rather than beforehand. Unethical suppliers need to be identified and shut down because they manage to stay in business today – even proliferate – as a result of there being no consequences for their actions. Better technologies are needed to track parts as they move through the supply chain, so that data can be shared with the industry at large to discredit unethical suppliers.

Some additional methods companies are using to detect counterfeit electronics include:

- Indentation & Marks
- Decapsulation
- Electrical Inspection
- X-Ray and SEM Inspection

Serialization: The most powerful weapon to fight counterfeiting

The most powerful technology in the battle against counterfeiting is serialization. Unique serial numbers are designated to each and every product through complex algorithms that originate from a separate database integrated with the manufacturer's production line. Serial numbers follow the product as it moves along the supply chain so it can be reliably traced back to the source. This form of Parent-Child serial number relationship provides a quick way to determine if the source is valid before it gets to its final destination, the customer. The serial number, which is a unique identification number similar to an automobile's VIN number, can be checked against a database to verify the product's authenticity from its origin.

These numbers are extremely difficult, if not impossible, for counterfeiters to duplicate. Considering the number of stops a normal package makes along the supply chain, serialization gives manufacturers, distributors, and shippers a much higher rate of confidence in the integrity of their electronic components. However, most manufacturers are ill prepared to adopt a serialization-based track-and-trace system due to a lack of standardization across the supply chain and not having a robust and automated labeling system in the first place.

Cloud-based labeling solutions: The first line of defense

In addition to the important question of authenticity, today's electronics product labeling requires a variety of complex information with data integrated from many data sources. Varied labeling governmental regulations and standards for new and existing markets, the need for speed due to new automation technologies in manufacturing, requirements for multiple languages, complex barcode data, and more — the real estate on a single label is populated with data from a variety of repositories. But many large companies are not managing this level of complexity with a reliable labeling strategy sophisticated enough to cover all these needs. It is understandable, then, that an attempt to serialize at the unit item level is putting the cart before the horse for many organizations.

Also, for affordable and effectively manageable security measures to be implemented in the supply chain, the ability to allow approved electronics supply chain suppliers and distributors to participate through a streamlined labeling solution is required. This secure access by authorized supply chain participants is the "first line of defense" against counterfeiting and diversion.

Standardization of barcode labeling solutions with approved suppliers and distributors can greatly diminish the likelihood of obsolete or counterfeit components making their

way into the supply chain. Cloud-based labeling solutions allow for secure access by approved suppliers and partners, as well as offering many other benefits to manufacturers. They also prevent mislabeling through the use of automation while offering support for regulatory data, multiple languages, and customer specific labeling requirements. In the end, labeling consistency and reliability is exponentially improved.

Standardization of barcode labeling solutions with approved suppliers and distributors can greatly diminish the likelihood of obsolete or counterfeit components. With serialization technology added to cloud-based labeling solutions, an unprecedented degree of security in tracking electronics components can save billions of dollars and prevent other safety concerns and environmental disasters.

The complexity of today's labeling requirements points to the fact that without the solid foundation of a good labeling strategy, customer dissatisfaction, returned shipments, counterfeits, and loss of business can accumulate, leading to significant erosion of revenue and profitability. Most importantly, the dangers of counterfeiting and diversion can have a negative impact on human health or even contribute to loss of life.

The Electronics industry is in an exciting phase of rapid expansion and change, and outdated labeling solutions are unable to keep pace with these dynamics. Fortunately, cloud-based labeling is one immediate way the Electronics industry can take charge in response to this changing environment. Such an approach allows organizations to be more responsive to the critical nature of the current labeling challenges and improve the stability of global supply chains, while concurrently stemming the dangerous rising tide of counterfeits.

To find out more about how Loftware's solutions can help you to overcome labeling challenges relating to counterfeiting and to see how electronics manufacturing organizations around the world benefit from an Enterprise Labeling approach, visit www.loftware.com.

Loftware™

The world's largest cloud-based Enterprise Labeling and Artwork Management provider

Locations worldwide:

- US
- Germany
- UK
- Slovenia
- Singapore

For additional resources, visit:

loftware.com/resources

Loftware is the world's largest cloud-based Enterprise Labeling and Artwork Management provider, offering an end-to-end labeling solution platform for companies of all sizes. Maintaining a global presence with offices in the US, UK, Germany, Slovenia, China, and Singapore, Loftware boasts over 35 years of expertise in solving labeling challenges. We help companies improve accuracy, traceability, and compliance while improving the quality, speed, and efficiency of their labeling.

As the leading global provider of Enterprise Labeling and Artwork Management, along with Clinical Trials Labeling and Content Management, Loftware enables supply chain agility, supports evolving regulations, and optimizes business operations for a wide range of industries. These include automotive, chemicals, consumer products, electronics, food & beverage, manufacturing, medical device, pharmaceuticals, retail, and apparel. For more information, visit www.loftware.com.

White Paper