Q) What’s the best course of action once you receive counterfeits? Who best to report to?
A) Any one of the organizations mentioned, including others like JEDEC should be told and most importantly, the original component manufacturer of the component needs to know.

Q) RE: Label Check: To copy a label is much easier than counterfeiting an IC. And: who ensures that the shipping box contains what the label states? There might be completely different parts delivered.
A) All OCMs have strict packing (shipping preparation), label, and product packaging procedures to ensure quality, safety, and security of the product being shipped. Any deviation from previously received shipments or inconsistency between label and product markings should be considered suspicious. As a minimum, the following should be diligently checked for received shipments:
1. Documentation
2. Outside Packaging (labels, box, tape, box markings and/or logos)
3. Inside Packaging (labels, packaging material, product box (OCM’s don’t use newspaper)
4. Product marking front and back (product name, lot number, date code, logo)
5. Remember, the analysis results of a few pictures or pieces cannot be automatically applied to the remaining pieces of a shipment which are not tested. Such analysis are inconclusive and potentially misleading.

There is also a label company that specializes in this issue: https://epsnews.com/2016/08/24/why-barcode-labeling-matters-in-electronics/

Q) How does one determine an Authorized Source?
A) Authorized, or franchised distributors can be found on the OCM’s website. You can cross check that by going to the distributor website and look for the OCM’s name. Aggregators are more difficult to determine. The only 100 percent authorized aggregator is ECIA authorized via ECIA.org.

Q) We were hit with a DIP IC that was marked one way and it was a completely different die.
A) That is a very common counterfeit situation. This can prove deadly in certain situations.

Q) How to get from Original manufacturers of obsolete IC, the correct markings and manufacturing marking, to check against inbound components?
A) This is a difficult situation, especially when dealing with obsolete IC’s. Many OCM’s will not provide such data (unless you are customs or enforcement agency) because it is this information that counterfeiters need, and actively search for, to create new counterfeit products. Some OCM’s “may” be open to providing support for such requests if detailed information on the product and source are provided. This is not a guarantee. Check if the OCM has an authorized partner specializing in managing and distributing obsolete product. Always remain cautious. If you are not sourcing from an authorized source, be aware that even CoC’s and documentation can be counterfeited.
Q) Does it make sense to have a label checked before delivery? It would be a great benefit to have a platform for this. Some manufacturers have this.
A) Every level of diligence is good but finding the components in the authorized channel (current and EOL parts) is always best, even though very difficult at times. Additionally, labels are easily copied one-to-one to near perfection. A perfect label doesn’t mean the product being shipped is a match. Remember, originality does not always equal reliability.

Q) Can Silicon Expert provide GIDEP or ERAI reports, not the file number only?
A) GIDEP does not allow us to release the actual document only the document number. Hopefully they will change that policy at some point.

Q) Who is more exposed, commercial or military/aerospace?
A) Both are at risk. A simple component in a cell phone that regulates the battery charging could be just as deadly as a counterfeit in a jet fighter. Mil/aero devices are higher prices, which is why they are frequently targeted.

Q) If the OCM can’t confirm if the product is authentic or not? As a customer how are we supposed to confirm the same?
A) - Establish strict procurement procedures that only allow authorized proven distribution channels. Product sourced outside these channels includes risk.
- Always ask for evidence for traceability, liability, and warranty!
- Some OCM’s “may” be open to providing support for such requests, if detailed information on the product and source are provided prior to verification. This is not a guarantee.
- Implement a Fraudulent Part Detection Plan. If you have previously purchased original product via authorized channels, create a database of pictures and information on the product, package, label, markings, and shipping materials. Any deviation from previously received shipments or inconsistency between label and product markings should be considered highly suspicious. As a minimum, the following should be diligently checked for received shipments:
  1. Documentation
  2. Outside Packaging (labels, box, tape, box markings and/or logos)
  3. Inside Packaging (labels, packaging material, product box (OCM’s don’t use newspaper))
  4. Product marking front and back (product name, lot number, date code, logo)
  5. Remember, the analysis results of a few pictures or pieces cannot be automatically applied to the remaining pieces of a shipment which are not tested. Such analysis are inconclusive and potentially misleading.

Q) Are there any forums to discuss clones or counterfeit components and types of effects on hardware
A) ERAI and SAE sponsor annual forums as do several other organizations. Also, a great place to start research on the latest news, info, and organizations combating counterfeiting is the Anti-Counterfeiting Forum (https://www.anticounterfeitingforum.org.uk/) / specifically: Organisations Combating Counterfeiting (https://www.anticounterfeitingforum.org.uk/other_sources.aspx#orgs)

Q) Always check your company’s legal before reporting
A) Yes, from a company perspective, check what is the best procedure and ensure management is informed… but it should NOT prevent reporting. If counterfeit is encounter and not reported, one could be considered complicit in the counterfeiting. REPORT, REPORT, REPORT!
Q) CLONED = Advanced Counterfeit devices! No such thing a cloned devices?
A) Yes, the phrase “advanced counterfeit devices” is a good way to describe clones. However, there are counterfeit parts that could be described as “advanced counterfeit devices” that do not fall into the category of clones. The word “clone” or cloned” is a term accepted by industry and government experts, companies, and individuals involved in anti-counterfeit to describe a specific category of counterfeit. A good article on clones is available on the IEEE Spectrum website: Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market

Q) How can you avoid the counterfeit if it is marked as per OEM? What are the end users’ techniques to adopt?
A) If the Original Component Manufacturer is marked on the part, then it should be coming from the authorized supply chain. If it has been re-marked with the OCM’s logo and found to be counterfeit, it needs to be reported so that others don’t spread in the supply chain. If sourced outside the authorized channel, there are no procedures that will ensure counterfeit can be 100% avoided.
- Establish strict procurement procedures that only allow authorized proven distribution channels. Product sourced outside these channels includes risk.
- Always ask for evidence for traceability, liability, and warranty!
- Some OCM’s “may” be open to providing support for such requests if detailed information on the product and source are provided prior to verification. This is not a guarantee.
- Implement a Fraudulent Part Detection Plan. If you have previously purchased original product via authorized channels, create a database of pictures and information on the product, package, label, markings, and shipping materials. Any deviation from previously received shipments or inconsistency between label and product markings should be considered highly suspicious. As a minimum, the following should be diligently checked for received shipments:
  1. Documentation
  2. Outside Packaging (labels, box, tape, box markings and/or logos)
  3. Inside Packaging (labels, packaging material, product box (OCM’s don’t use newspaper))
  4. Product marking front and back (product name, lot number, date code, logo)
  5. Remember, the analysis results of a few pictures or pieces cannot be automatically applied to the remaining pieces of a shipment which are not tested. Such analysis are inconclusive and potentially misleading.

Q) Seriously, you test 100% of the components? Isn’t it cheaper to discard the lot and replace it.
A) One must also estimate the cost of risk for not testing 100% and unknowingly integrating counterfeit into hardware or systems. In such cases, it is then cheaper to test 100%. The best bang for your buck, (quality, reliability, assurance, warranty, customer satisfaction) is sourcing product via authorized channels.

Q) How much of a problem are counterfeits outside of the semiconductor industry, such as connectors and printed circuit boards?
A) Essentially, if there is money to be made easily by counterfeiting something, it’ll happen. This includes PCBs that are poorly made.

Q) Is there an industry resource that maintains an authorized source matrix for all manufacturers?
A) All manufacturers list their authorized distributors on their website. Always start there!
Also, ECIA.org has one for authorized distributors, but only ECIA members
Q) The bigger concern with reporting is a reluctance to report unless one is absolutely sure parts are counterfeit - frequently they are suspect, but since OCM’s are reluctant to evaluate, we cannot be sure.

A) True. But ERAI will keep that information confidential until after a part has been tested and determined to be counterfeit. They aren’t interested in false accusations; they’re interested in identifying actual counterfeits and dispersing the information. But be assured, OCM’s evaluate information reported. It is the foundation of their anti-counterfeiting operations. For liability reason, OCM’s are not keen on verification of non-traceable product or for the purpose of selling or sourcing via non-authorized channels. Every situation is unique. Reach out to the OCM in question and discuss your concerns. Many OCM’s website provides a telephone number or email for their anti-counterfeiting department. If this cannot be found, contact customer or tech support and ask to be put in touch with the department that handles counterfeit.

Q) How can you determine a part is authentic?

A) The best way is to procure the part from the authorized supply chain that will come with a Certificate of Conformance, etc. If it has come from the Independent Distribution channel or a broker, there needs to be thorough testing and research to make sure the parts are authentic.

Q) How is a clone different than a re-marked device?

A) A clone can use excess inventory and package could be ‘original’ as opposed to an existing, packaged part that has been blacktopped and re-printed. A good article on clones is available on the IEEE Spectrum website: Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market

Here is a short excerpt from the article:
“...unlike counterfeit electronics of the past, modern clones are very sophisticated. Previously, counterfeiters would simply re-mark or repackage old or inferior components and then sell them as if they were new and top of the line; the main problem with these knockoffs was poor reliability. Cloned electronics these days are potentially more nefarious: The counterfeiters make their own components, boards, and systems from scratch and then package them into superficially similar products. The clones may be less reliable than the genuine product, having never undergone rigorous testing. But they may also host unwanted or even malicious software, firmware, or hardware—and the buyer may not know the difference, or even know what to look for.”

Q) How can DNA or others really help if parts are only “remarked”? DNA would be still genuine...

A) If used, specific DNA would be for a specific product. DNA marking does not come at the OCM level—it is applied after the part leaves the factory. That has been the main criticism of DNA in the electronics supply chain.

Q) RE: Label Check: To copy a label is much easier than counterfeiting an IC. And: who ensures that the shipping box contains what the label states? There might be completely different parts delivered.

A) Very true. This happens often.

Q) Who are these counterfeit manufacturers? It takes a big investment to set up a fab. Do the counterfeit manufacturers find the funds to do this?

A) There is no fab involved. They take existing components or excess and convert it to counterfeit parts. To gain a solid understanding of the where, why, and how of semiconductor counterfeiting, read The World Semiconductor Council White Paper: Winning the Battle Against Counterfeit Semiconductor Products
Q) If we perform electrical stress tests over and over again, are we reducing the life of components? Tests include shock, vibe, low and high temp, ... SAE specs states that these tests may be “life limiting”
A) The OCM’s do this for you. Purchases need to be made via authorized channels.

Q) What happens if a CofC is received and/or test results pass ... however we detect this as a counterfeit part / lot?
A) Each case is obviously unique, but has the testing been done on the entire batch? And, refer to the originator of the CofC to make sure that is not counterfeit. CofC’s are counterfeited as much as the actual components.

Q) Visual inspection ... can we also find out an unsafe source / unclear situation based on information on the labels?
A) Yes. Diligence should be at every stage of procurement.