Counterfeit Semiconductors and the Online Environment

World Semiconductor Council

June 4, 2021

Introduction

The online environment as a commercial marketplace has revolutionized consumption and provided huge opportunities for businesses to grow their reach to consumers internationally. In parallel, however, the online environment also has significantly increased the counterfeiter's ability to expand their illegal activities and reach greater numbers of potential unsuspecting customers. Counterfeits covering all legitimate products including semiconductors are available through many online intermediaries such as legitimate websites, e-commerce market platforms and via social media networks and apps. The dynamic internet space has become particularly vulnerable to counterfeiters. The era of COVID-19 has also accelerated counterfeiting. The combination of the online economy and globalization has created a perfect environment for counterfeiters to function, allowing them to sell all goods directly worldwide with virtually no barriers to entry, low cost of set up, easier distribution and much fewer risks of being caught.

As is well documented in the World Semiconductor Council (WSC) White Paper, "Winning the Battle Against Counterfeit Semiconductor Products ," counterfeit semiconductors pose major threats to the health, safety, and security of everyone that relies on electronics.[1, 2] Due to the dangers posed by counterfeits, the WSC has an anti-counterfeiting task force working to promote anti-counterfeiting activities, including training and sharing relevant information with enforcement authorities, raising awareness, and encouraging purchases from authorized sources. This paper builds on these awareness raising activities.

Current Status of Counterfeit Semiconductors & Online

The semiconductor industry is impacted by the availability and offering for purchase of counterfeit or trademark infringing semiconductors online. Most counterfeit semiconductors are increasingly offered via various internet platforms and online sources. Counterfeiters can now

[1] http://www.semiconductorcouncil.org/wp-content/uploads/2018/06/WSC-Anti-Counterfeiting-White-Paper-May-2018-Update.pdf

[2] White Paper cites counterfeit case examples destined for, automated external defibrillators, IV drip machines, automotive and high-speed train braking systems, airbag deployment systems and airport runway landing lights.

advertise products with relative ease and anonymity. Value chain actors looking for genuine products can become victim to counterfeit websites or counterfeit advertisements that use partly legitimate information like accurate product pictures to mislead potential customers. The typical online channels for offering semiconductor counterfeits for purchase are:

- E-Commerce platforms
- Online marketplaces
- Online advertisements linking to specific illegitimate sources
- Rogue web shops

The online counterfeiting industry business model, which largely relies on online platforms and tens of thousands of stand-alone websites, continues to be a dynamic environment. The model has also in some areas partly shifted to facilitating sales links through social media platforms, instant messaging tools and apps. There are also indications that trademark infringing offerings on the big online platforms may be decreasing in recent times and have shifted from the large well known B2B & B2C platforms to less well-known platforms.

Regulatory Developments

The nature of the internet trade in counterfeit products has made combating counterfeiting and enforcing IPR online effectively a very challenging global issue for all stakeholders. The combination of consumer reach and anonymity of selling online also creates a challenging environment for enforcement authorities. Regulatory authorities have published various watch lists outlining physical and online markets that have been identified as facilitating counterfeiting and piracy.[3] Authorities now are trying to increase the responsibilities of those intermediaries and e-commerce platforms active online. In 2019, China implemented legislation *(E-Commerce Law)* that holds e-commerce platforms jointly accountable for the sale of counterfeit products with the parties marketing such counterfeits on their sites. This new legislation requires online retailers to act quickly once a breach has been reported. In 2020, the European Union proposed draft legislation *(Digital Services Act)* which includes provisions detailing the 'Know Your Business Customer principle' (KYBC), whereby online marketplaces will be required to verify the identity of sellers. The proposal includes new obligations for very large platforms to take risk-based measures to prevent misuse of their systems and rules for removing illegal services and counterfeit goods and rules to ensure that sellers of counterfeits can be detected more quickly.

[3] https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159183.pdf
https://ustr.gov/sites/default/files/files/Press/Releases/2020%20Review%20of%20Notorious%20Markets%20for%20Counterfeiting%20and%20Piracy%20(final).pdf

Mitigation Practices

The implementation of strict procurement practices for customers remains the best way to protect against counterfeit semiconductors that are offered online finding their way into the overall electronics chain. Original Component Manufacturers (OCM) sell their semiconductor products in two ways: directly from the original manufacturer and through their authorized distributors. Original Equipment Manufacturers (OEMs) and their Contract Manufacturers (CMs) that procure components exclusively through authorized sources, including authorized aftermarket distributors/manufacturers, will also eliminate the need to conduct costly, time-consuming, and error-prone authenticity testing. The authorized distributors for a given OCM can be easily found on the OCM's website.

OCMs should also perform structured internet searches for evidence of IPR infringing sale offers. Additionally, OCMs should make regular use of the procedures now offered by e-commerce platforms and online marketplaces to de-list or take down IP infringing listings and sales offers.

3rd party service providers are active in offering support to semiconductor companies for monitoring and enforcement of rights of semiconductor trademark owners related to counterfeit semiconductor offerings via online platforms.

Conclusion

The online economy has created a perfect environment for the anonymous sale of counterfeit semiconductors directly worldwide. These online counterfeits pose major threats to the health, safety, and security of everyone that relies on electronics. Governments are trying to respond by publishing watch lists of markets that facilitate counterfeits, requiring online retailers to act quickly to reports of counterfeits, and considering a 'Know Your Business Customer principle' (KYBC) for online marketplaces to verify the identity of sellers. OCMs should consider having their own company program in place to address the potential sale of counterfeit semiconductors online and should use the appropriate mitigation tools to assist authorities and platforms to detect IPR infringing offers. OEM manufacturers can do their part to avoid counterfeits by purchasing directly from the original semiconductor manufacturer and through their authorized sources.