AGMA GLOBAL
Advancing Intellectual Property Protection

FOR IMMEDIATE RELEASE

Media Contact:
Stephanie Olsen
Lages & Associates
(949) 453-8080
stephanie@lages.com

Employee Training, Reporting Mechanisms Identified by AGMA as Crucial Components in Fight Against Warranty, Service Abuse

Non-Profit Technology Consortium Continues Series of Best Practices for Successful IP Protection

LOS GATOS, Calif., February 26, 2019 – Though it may seem like a minor issue – a faked warranty claim here, service received for an expired plan there – the use of services and support without proper entitlement or authorization is a huge threat to technology OEMs and service providers everywhere. Known as service abuse, these and other similarly shady practices can lead to billions of dollars in lost revenues each year, and negatively impact customer confidence, company reputations and more. AGMA, a non-profit organization and the largest group solely focused on intellectual property protection in the high-tech industry, is offering a series of best practices that are geared towards protecting brands. Having identified contract provisions as a first step, AGMA is now pointing to a one-two punch of education and action as the next tactic in the fight to put service abuse perpetrators on the ropes.

A rapidly growing concern, service abuse can be enacted by nearly anyone who has dealings with a business – from unethical end users to business partners and distributors. A problem this broad in scope calls for an ever-vigilant detection system, and employees should be placed on the front lines. Service and warranty abuse is a crime – and anyone who experiences it has an obligation to report it. It is up to the OEM or service provider to make reporting these offenses simple and free from repercussions to the reporting party.

Detecting Fraud

Because people can't report what they don't know, education on what service and warranty abuse is, what it looks like, and what to do about it is critical. A thoughtful, detailed training process for both internal employees and the external channel partner population should be implemented, with content that is tailored to each audience.

New hires should receive training within the first 90 days of their hiring and company-wide refresher sessions held at least yearly. Training sessions should be recorded, making them easy to view on demand. Additionally, because the content of these sessions can become obsolete quickly, any training sessions that have dated content should be refreshed and updated to reflect current policies.

A second, complementary method of identifying wrongdoings is to employ one of the many relevant tools on the market that utilize big data analytics. By capturing data related to services and warranties and analyzing it against relevant metrics (such as countries of origin, expected number of replacement parts, etc.), red flags can be revealed. Any anomalies found can trigger further questioning and spur investigations that take a deeper look into channel partners or resellers that regularly display such inconsistencies.

Reporting Mechanisms

In keeping with the Department of Homeland Security's mantra of 'If you see something, say something' – after fraud is identified, it needs to be reported. It is essential for brand owners to have an easy, anonymous method in place for people to report issues that affect the company. Typically, this will be via a generic internal email address, which is then routed to the correct department. Company portals can also provide a path for reporting.

Reports of suspected wrongdoings can originate from both inside the company itself and from outside 'whistleblowers.' Oftentimes, people communicating via the brand owner's designated reporting system do not want to be broadly identified for fear of retaliation, making it important to treat these communications with confidentiality. In order to foster an environment that encourages people to come forward, they must be made to feel comfortable in reporting what was seen.

"It's often said that the best defense is a good offense, and that is especially true when it comes to combating service and warranty abuse," noted AGMA president Sally Nguyen. "Companies that address these issues can generate enormous savings and create long-term value for their organizations, their investors and their customers, without compromising customer service and satisfaction. Our mission at AGMA is to ensure that technology companies have access to the insights and best practices needed to effectively address service abuse – as well as a broad range of other brand protection issues."

As an industry association, AGMA is chartered with addressing key threats to intellectual property in the high-tech industry. To learn more about AGMA, please visit www.agmaglobal.org.

About AGMA

AGMA is a non-profit organization comprised of influential companies in the technology sector. Incorporated in 2001, AGMA's mission is to address gray market fraud, parallel imports, counterfeiting, software piracy, and service abuse of technology products around the globe. The organization's goals are to protect intellectual property and authorized distribution channels, improve customer satisfaction and preserve brand integrity.

AGMA welcomes technology manufacturers, as well as persons or entities that own or hold intellectual property rights to finished goods outside the technology industry; government and law enforcement officials; product and service providers who provide goods and/or services to combat gray market fraud, counterfeiting and warranty and service abuse threats. AGMA uses a variety of avenues to cultivate change in the marketplace, including event speaking, educational initiatives, benchmark studies, industry guidelines, and, where appropriate, public policy advocacy. To learn more about AGMA's initiatives or to become a member, please visit www.agmaglobal.org or follow them on LinkedIn and Twitter.

# # #