Expand Your Markets: Keep Your RFID Business Safe from the FCC and International Enforcement Agencies

Ronald E. Quirk, Head of IoT Group

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

DISCLAIMER: This presentation is intended for informational purposes only and is not for the purpose of providing legal advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a lawyer if you want legal advice. **No attorney-client or confidential relationship exists or will be formed between you and Marashlian & Donahue, PLLC, The *Comm*Law Group, or any of our representatives.**

MARASHLIAN & DONAHUE, PLLC
THE *COMM*LAW GROUP

FCC's Brave New World of RF Equipment Enforcement

- The FCC has recently commenced enforcement actions against numerous RF equipment stakeholders:
  - *$144,344 fine on RF equipment dealer that advertised non-compliant audio/visual transmitters for sale on its website.*
  - *$25,000 fine on a company that marketed fluorescent lighting ballasts that did not have the FCC logo affixed to them.*
  - *$90,000 fine on a manufacturer of LED light fixtures for marketing devices that caused interference to radio operations.*
  - *$90,000 fine on manufacturer of unlicensed national information infrastructure ("U-NII") devices for marketing devices without the required security features.*
  - *Fried chicken restaurants in Texas sanctioned for operating outdoor LED signs that emitting RF energy that threatened airport communications two miles away.*
  - *FCC prosecuting Brooklyn man for operating a Bitcoin miner that purportedly interfered with T-Mobile's LTE network – case could end with fines of over $100,000 levied on operator and manufacturer.*

Fines are but One Issue

- Most FCC enforcement actions are done publicly, harming the reputations of the accused companies.
- FCC typically requires companies to cease selling offending devices.
  - *This can include ordering manufacturers and vendors to take all such devices off the market, disconnect and disable operating devices. And even, in cases involving underground equipment, out of the ground.*
- During the past year, the FCC has added a new wrinkle to enforcement proceedings: threatening to hold hearings to revoke the certifications of equipment manufacturers and importers that violate FCC rules, effectively banning them from marketing their products in the U.S.

Fines Themselves can be Steep

- Communications Act Section 302a(b)
  - *Prohibits the manufacturing, sale, offering for sale (including advertising), importation, shipping, or operation of RF devices that violate FCC rules.*
- Communications Act Section 501
  - *$10,000 base fine for willful violation of the Act.*
- Communications Act Section 502
  - *$500 per day for willful violation of FCC rules.*
  - *Each noncompliant device sold is a separate violation.*
  - *Each rule violated is a separate violation.*

FCC Rules for RFID Systems

- RFID equipment is mainly regulated under Parts 2 and 15 of FCC rules governing authorization, operation, and marketing low power RF devices.
- RFID systems are “secondary” spectrum users.
  - *Must not cause harmful interference to other wireless operations.*
    - FCC lists emissions limits for unlicensed frequencies in Part 15, based on frequency band used.
    - If RF emissions limits are exceeded, system must be shut down until problem is resolved.
  - *RFID systems have no interference protection from other wireless operations.*
  - *RFID systems must operate on authorized frequencies.*
    - FCC lists restricted frequencies in Part 15.
    - Operation on unauthorized frequencies is a violation of the FCC’s rules.

RFID Regulatory Classification

- Because RFID readers transmit low power radio waves, the FCC classifies them as “intentional radiators.” RF devices that do not transmit RF energy are typically classified as “unintentional radiators” or “incidental radiators.”
- With certain exceptions (e.g., trade shows, testing, sales contracts), the FCC requires that all intentional radiators be certified and properly labeled prior to marketing or operation.
  - *Certification procedures*
    - Responsible party submits a prototype to a lab for compliance testing. Required documentation must include information as to the category and subcategory of the device, and which FCC rules apply.
    - Once tested and approved, the device and applicable documentation must be submitted to a Telecommunications Certification Body (TCB) for FCC certification.
    - Once certified, the device must be properly labeled and applicable consumer information provided to the user.
    - Certifications and testing information are made public via the FCC’s website. Confidentiality must be requested when device is submitted to the TCB.

Responsible Party

- FCC rules state that the party responsible for FCC compliance of an intentional radiator is the entity that seeks certification of the device. This is typically the manufacturer, importer, or distributor.
- The responsible party is basically required to ensure the device meets FCC specs when it is sold and operated, unless the device is modified in an unauthorized manner.
  - *In that situation, the entity that modifies the device becomes the responsible party.*
  - *But, if the device can be easily modified by the user, the original responsible party is on the hook if the device is used improperly. This typically occurs when a device, such as the Bitcoin miner previously discussed, enables the user to easily change frequencies and operate on unauthorized channel.*
- While end-users are typically not the responsible party, they can still be held liable for operating RF equipment in violation of FCC rules. In order for that to occur, the responsible party must clearly inform customers in user manual or elsewhere (e.g., website, as long as the customer is notified how to access the information) the conditions under which the device may be operated. If, for example, the device is authorized for use in industrial areas, the user must be informed that it cannot be operated elsewhere

Post Market Surveillance

- Last year, the FCC promulgated and commenced enforcing new RF equipment rules. One of the most important new rules is that the FCC has codified the requirement that TCBs must conduct post market surveillance on at least 5% of the devices it certifies within a given year.
  - *TCBs conduct post market surveillance by purchasing or requesting a sample device that is on the market, examine and test it for compliance. If the device is non-compliant, an enforcement proceeding is initiated against the responsible party.*

FCC Trolling

- The FCC actively monitors websites of RF equipment manufacturers and distributors to determine compliance with FCC rules.
  - *FCC rules required proper labeling and indication of FCC authorization on RF equipment advertisements.*
  - *If a website does not list such information, the FCC can, and often does, commence an enforcement proceeding. The AV equipment supplier discussed earlier was caught via FCC website trolling.*
  - *All responsible parties must ensure that FCC compliance information is displayed in their advertising.*

New Rules

- In addition to post market surveillance, the new FCC rules provide for:
  - *New self-approval authorization techniques for unintentional radiators.*
  - *Streamlining of RF equipment importation rules.*
  - *Specific requirements for electronic labeling of RF devices.*
  - *New measurement procedures and standards.*
- The FCC plans to promulgate additional rules in subsequent proceedings.
  - *New responsible parties for refurbished devices.*
  - *Stringent software security requirements.*
  - *New rules concerning confidentiality of information contained in RF equipment certification applications*

Best Practices

- The FCC is watching RF equipment suppliers like a hawk. Hence, all RFID equipment suppliers are well advised to have regulatory best practices to ensure FCC compliance and market their products without fear of FCC enforcement. Best practices include:
  - *Understanding and complying with all pertinent FCC rules and keeping up on changes to them.*
  - *Correctly categorizing and equipment and properly testing and authorizing same.*
  - *Vendor contract practices:*
    - Warranties that equipment is FCC compliant and compensation for down time.
    - Clarify how equipment is to be marketed and consumer information provided – no warranties for violations.
    - Indemnify in event of third party lawsuit involving interference.
    - Lab performing tests should be identified – beware foreign labs.
  - *Advertising & marketing practices.*
  - *Importation and working with foreign components.*
  - *Efficient legal guidance before the FCC Enforcement Bureau & mitigating legal liability.*
  - *Legally expanding markets overseas.*
  - *Privacy protection (for information contained on tags).*

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Expanding Markets Overseas

- Importing and marketing RFID equipment in foreign countries can be daunting.
  - *Equipment authorization procedures vary greatly from country to country.*
  - *Plan well in advance of your proposed sales in foreign countries.*
    - Some countries will authorize equipment within a matter of a few weeks. Some take several months to complete the authorization process.

Testing Procedures

- The first step in obtaining authorization is testing for compliance with the country's technical specifications.
  - *Some countries (e.g., Vietnam & Brazil) require in-country testing of RF devices as part of the authorization procedure. This can significantly increase the costs and slow the timeframe for authorization.*
  - *Other countries (e.g., Sri Lanka, UAE, Honduras, India) will accept FCC or CE test reports (typically EU test), as long as they conform to those countries' standards.*
    - A typical procedure is to submit samples to a testing lab and have the lab prepare test reports for individual countries.
  - *If a device is going to be marketed in the EU, test reports showing compliance with all the applicable directives and CE Mark requirements is mandatory.*
  - *Make sure the lab you choose is certified and reputable. Unreliable test reports can result in enforcement actions and steep fines.*

Boots on the Ground

- Once your device is tested, finding a reliable in-country consultant is critical.
  - *Foreign governments often require local contacts to process authorization applications and act as points of contact if regulatory matters arise.*
  - *A good consultant will spell out the exact requirements, provide a quote, know the right government officials, coordinate testing, provide a realistic timeframe, do all the filing and follow-up work, and be willing to perform workarounds to expedite service if any are available in a given country.*

Know the Current Rules

- Foreign countries are known to change their RF equipment rules with little public notice. It is important that your consultant keep up on the current rules.
  - *China recently streamlined its rules so that RFID readers are now subject to a lot less scrutiny than they used to be.*
  - *Other countries have RF authorizations that expire after a given period of time; if renewals are not timely filed, the whole authorization process must be repeated.*

Labeling

- Each country has its own RF equipment labeling requirement. Your consultant should inform you of the exact requirements and ensure that all your marketed devices are properly labeled.
- Improper labeling or lack of labeling is the first thing the authorities look at to determine rule violations.

Importation

- Most countries require full authorization before permitting RF equipment to be imported. There are often exemptions for limited quantities imported for exhibiting or experimental purposes.
- Be sure you have an Importer of Record in each country. They are mandatory in most countries. IoRs will ensure that your products get through customs, warehouse your equipment if necessary, and will act on your behalf should problems arise.

Best Practices for Foreign Sales

- For reasons similar to those regarding FCC compliance, it is critical for companies selling overseas to implement best practices.
  - *Our firm specializes in international RF equipment matters. We understand what needs to be done. And, we work directly with vendors who have in-country representatives to assist with efficient regulatory compliance.*
    - We have a Global RF Equipment Compliance Guide for sale that provides a great deal of information. Samples are available here, and we offer conference attendees 50% off the retail price of the full guide.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

THANK YOU

MARASHLIAN
& DONAHUE, PLLC
THE COMMLAW GROUP