

How the FCC Enforces Part 15

By Glen Dash

Note: Material may be dated.

For more information go to:

www.glendash.com/dated_material

To understand the FCC's regulations, it is necessary to know how the FCC enforces them. The commission has an active enforcement program that comprises a wide range of potential penalties. For many manufacturers, a basic quality-assurance program to assess the potential effects of equipment modifications and monitor EMI performance can prevent problems. Consider the following:

- Every fall the FCC sweeps through the COMDEX computer exhibition in Las Vegas. FCC investigators typically assess fines totaling \$400,000 or more on hundreds of manufacturers that run afoul of the FCC's marketing rules.
- The FCC can levy large fines. In the early days of the FCC's Part 15 program, the fines were minimal, but in 1990 Congress increased the commission's fining authority 15-fold.
- The commission's compliance campaign targets marketers and end users as well as manufacturers. FCC personnel have visited computer stores around the country and fined them for selling uncertified Class A computer equipment to consumer end users. The commission has been known to purchase lists of trade-show attendees in order to target inspections for non-compliant equipment, on which it could impose cease-and-desist orders.
- The FCC can reach out to foreign violators of its rules by denying entry at U.S. Customs.

This program makes compliance both an economic and a legal necessity. An understanding of how the FCC enforcement program operates is essential.

Background

The FCC's 1979 EMI regulation of digital equipment was triggered by interference to broadcasting and other radio services. In Nevada, an errant vending machine interfered with highway patrol operations on 42 MHz. Aeronautical communications in the 113 MHz band were also disrupted, as were land mobile services at lower frequencies.

The FCC's concern was well founded. Every year, the FCC processes some 55,000 interference complaints, of which approximately 10% concern Part 15 equipment. With the dramatic growth in computer-based equipment, careful regulation has become necessary to limit interference.

Until recently, the FCC's regulatory efforts were focused on makers of Class B equipment. The FCC has now begun looking to see if Class A equipment manufacturers are complying, and plans are under way to step up enforcement of the Class A specifications as well. In taking these measures, the FCC is seeking not to root out inadvertent violators but rather to be responsive to complaints from end users and competitors.

Two situations are likely to trigger an FCC examination. First, if an end user complains that equipment is causing interference, the FCC will likely respond. Second, if a competitor complains that he or she has been put at a competitive disadvantage by complying with the FCC rules, the commission will also take action.

The FCC's Enforcement Procedure

The most likely sanctions for the FCC to impose are the "administrative remedies" laid out in Title 47, Section 503(b), of the U.S. Code. The document describes a two-step process.

Base Forfeitures		
Violation	% of Statutory Maximum	Monetary Amount
Misrepresentation/lack of candor (e.g., making false statements on FCC Form 731 or on an equipment-authorization application)	80	\$8,000
Failure to comply with prescribed markings (e.g., incorrect equipment labels or user-manual statements)	80	\$8,000
Operation without an instrument of authorization (e.g., pre-compliant device operation at trade shows without the required notice)	80	\$8,000
Unauthorized substantial transfer of control (e.g., transferring a grant without FCC approval)	80	\$8,000
Failure to respond to commission communications	70	\$7,000
Importation or marketing of unauthorized equipment	70	\$7,000
Use of unauthorized frequency	50	\$5,000
Use of unauthorized equipment	40	\$4,000
Operation at an unauthorized location (e.g., Class A equipment in Class B environment or exempt industrial control equipment in a commercial environment)	40	\$4,000
Failure to file required forms or information	30	\$3,000
Failure to make required measurements	10	\$1,000
Failure to maintain required records	10	\$1,000

TABLE 1: The FCC sets forfeiture penalties, or fines, according to the type of infraction and its table of adjustments. Shown above are starting points for some common rule violations.

Adjustment Criteria

Violation	Adjustment to Base Amount
Egregious misconduct	+50–90%
Ability to pay/relative disincentive	+50–90%
Intentional violation	+50–90%
Substantial harm	+40–70%
Prior violations of same or other requirements	+40–70%
Substantial economic gain	+20–50%
Repeated or continuous violation	Varies
Minor violation	-50–90%
Good faith or voluntary disclosure	-30–60%
History of overall compliance	-20–50%
Inability to pay	Varies

TABLE 2: The base amount is adjusted upward or downward in response to case-specific factors, giving the commission wide latitude.

First, the FCC can issue a “Marketing Citation,” a letter informing the company that it is apparently violating FCC rules, and perhaps requesting that a product sample be sent to the FCC laboratories. If the violations continue or if the equipment is found to be in technical violation of the rules, a “Notice of Apparent Liability” will be issued. This letter is roughly equivalent to an audit letter issued by the Internal Revenue Service. It can assess a fine of up to \$10,000 for each occurrence and up to \$75,000 per violator for multiple occurrences. Congress raised the fines in 1990 from \$2,000 and \$5,000, respectively, to strengthen the FCC’s hand.

The FCC can exercise discretion in assessing the fines. In order to provide consistent treatment of different violations, the commission considers two factors. A basic amount is assigned for each type of offense, and an adjustment is applied where mitigating or aggravating factors are involved (see Tables 1 and 2).

Manufacturer fines are not the FCC’s only administrative weapon. The commission can also hold up processing of all pending applications and can move against a manufacturer’s customer base with fines, disrupting its business relations. Section 503(b) applies to “any person who is determined by the Commission... to have ... willfully or repeatedly failed to comply with any...rule, regulation, or order issued by the Commission.” Because the regulation applies to any person, and not just any manufacturer, the commission can notify a manufacturer’s distributors, or even its end users, that the device in question does not comply with FCC rules and that if they continue to use the product, they can be held liable for the same fine assessed against the manufacturer. Using the coercive power of Section 503, the commission can simultaneously notify recalcitrant manufacturers, their distributors, and their customers that a product is not compliant and threaten all of them with fines. This wholesale use of Section 503 has been known to bring sales to a standstill. In fact, approximately two-thirds of the Marketing Citations issued by the commission go to distributors and users, not to the manufacturers themselves.

Another mechanism of expansive enforcement is the use of a Public Notice. The commission can, without a prior hearing or notice, issue a Public Notice that a device has been found to be noncompliant. Such notices are circulated widely and reported in the media.

The issuance of Marketing Citations, Notices of Apparent Liability, and Public Notices is at the discretion of the FCC. All of these are “administrative remedies.” Powerful though they are, there will be some cases where stronger measures are required.

Going to Court

In these instances, the commission will seek out the "judicial" remedies of Sections 501 and 502. These are criminal penalties. To use them, the FCC has to employ the resources of the Justice Department, which will determine whether the commission has supplied it with enough information to establish a prima facie case that the rules have been willfully and knowingly violated. Title 47, Section 501, states that "any person who willfully or knowingly does...any act, manner, or a thing, in this chapter prohibited or declared to be unlawful...shall, upon conviction thereof, be punished for such offense...by a fine of not more than \$100,000 or by imprisonment for a term not exceeding one year." Note that this imprisonment term applies only to the first conviction; multiple offenses can carry higher penalties.

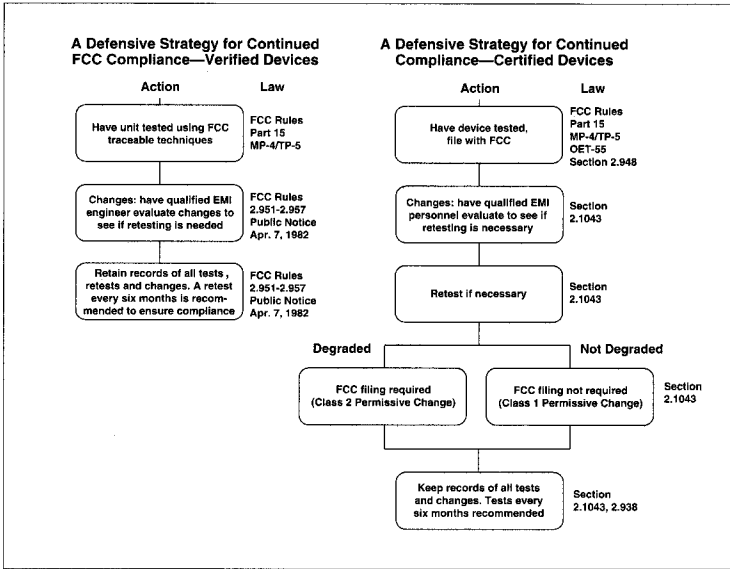


FIGURE 1: A strategy for compliance.

Since the Part 15 rules are primarily technical, the only real protection a manufacturer has against the possibility of FCC sanctions lies in proper testing of hardware.

A Plan for Compliance

For makers of both Class A and Class B computing equipment, the first essential step in protecting their company is to test the equipment properly. Only the loosest regulations govern the activities of test laboratories, and because of this, the commission tends to rely on its own test results in determining who should be sanctioned. Furthermore, once a company understands what's expected of it in terms of testing, it must preserve its compliant stature.

Class A Equipment

For Class A equipment, Section 2.955 specifies that the manufacturer must retain certain records, including 1) "a record of the original design drawings and specifications and all the changes that have been made that may affect compliance" (emphasis added), and 2) "a record of the procedures used for production, inspecting and testing (if tests were performed), to ensure conformance (statistical production line emission testing is not required)" (emphasis added).

These records shall be retained for two years after the manufacture of the equipment has been discontinued. The commission additionally has the right to review the records and to request a sample of the equipment.

With regard to changes, the commission issued a Public Notice on April 7, 1982, stating that

the manufacturer is cautioned that many changes which on their face seem to be insignificant are, in fact, very significant. A change in the layout of a circuit board or the addition, removal or rerouting of a wire, or even a change in logic, will almost surely change the emission characteristics (both conducted and radiated) of the device. This is particularly true with a device housed in a non-metallic enclosure. Whether this change in characteristics is enough to throw the product out of compliance can best be determined by retesting.

Taken together, these sections and the April 7, 1982, Public Notice add up as follows. The equipment should be tested by a laboratory using procedures identical to those used by the commission. Documentation of what equipment was tested (in the form of photographs, mechanical drawings, and schematics), as well as how it was tested, especially with regard to the arrangement of peripherals and cables, must be kept on file. Certain foreign governments require statistical production-line testing; fortunately, the commission does not. Nonetheless, to ensure continued compliance, it is advisable to test at least annually.

When changes are made (a nearly continuous process at many firms), the April 7, 1982, Public Notice implies that retesting is the preferred action, though the frequency of such changes may make retesting impractical. Here, one strategy is to have the most senior engineer involved with EMI compliance—preferably someone who has been trained in RF design techniques and testing—placed on the Engineering Change Order checkoff list. He or she can then decide whether the equipment can be modified without retesting, or whether emissions may have altered due

to the change, necessitating more testing. In this way, a responsible person, using his or her professional judgment, makes the determination as to whether additional testing is needed. Note, however, that this person could be liable for noncompliance, especially if he or she knowingly allowed a change to be made that

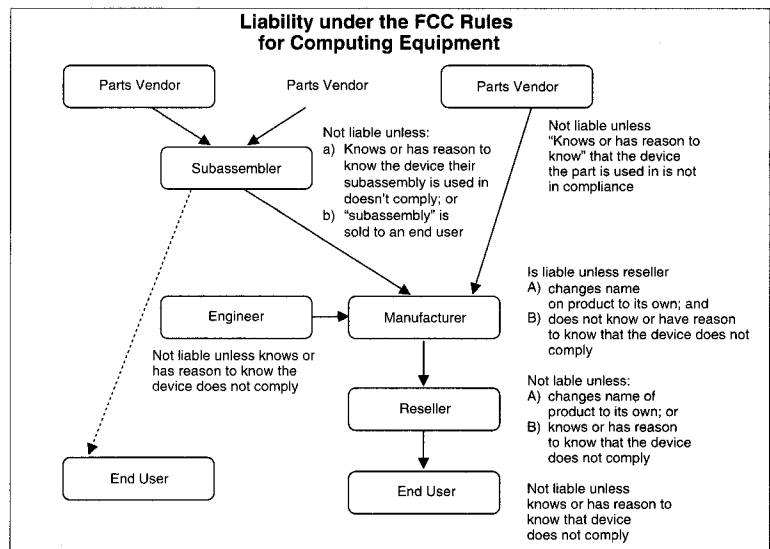


FIGURE 2: The chain of FCC liability.

would likely cause the device to emit emissions levels above those allowed by the regulations.

These Engineering Change Orders, along with the original test results and the results of any subsequent tests, should be kept on file should the FCC Field Operations Bureau call. Careful cataloging of this information can, in many cases, resolve any concerns the FCC may have.

Class B Equipment

For makers of Class B equipment subject only to verification, the same strategies should be used as for Class A equipment. However, Class B home computers and their peripherals are

subject to certification and must follow the scheme specified in Section 2.1043 of the commission's rules.

This section sets up a system of two classes of "permissive changes." A Class 1 Permissive Change includes any modifications to the equipment that do not degrade the characteristics reported by the manufacturer to the commission when certification was granted. No filing with the commission is required for a Class 1 Permissive Change.

By contrast, a Class 2 Permissive Change

includes those modifications which degrade the performance characteristics as reported to the Commission at the time of initial certification. Such degraded performance must still meet the minimum requirements of the applicable rules. When a Class 2 Permissive Change is made by the grantee, he shall supply the Commission with complete information and test results of the characteristics affected by such change. The modified equipment shall not be marketed under existing Grant of Certification prior to acknowledgment by the Commission that the change is acceptable.

Manufacturers should also note that the FCC has been tightening its interpretation of what changes can be considered permissive, regardless of their effect on emissions. Changes in CPU clock frequencies, for example, are not allowed under the permissive-change rules; instead, a new certification application must be filed (2.1043[a]).

Manufacturers of Class B certified equipment (personal computers and peripherals) must follow the same procedure as manufacturers of verified equipment in evaluating the EMI impact of equipment changes. If the changes are considered insignificant, the responsible RF engineer should sign off on them in the Engineering Change Order; if he or she is uncertain of their impact, the device should be retested. If the device's emissions are not degraded, careful records of the change and the emissions test should be kept. However, if emissions characteristics are degraded, an application to the FCC must be made and a grant authorizing the Class 2 Permissive Change received before the modified device can be marketed.

In any event, with Class B as with Class A devices, retesting is advisable at least annually, and preferably semiannually.

The Chain of Responsibility

Keep in mind that each case is different; to determine the exact nature of your company's potential liability, you will need to consult an attorney.

Under the FCC rules, Parts 2.805 and 2.803, computing devices "must comply with the specified technical standards

prior to use, [and] no person shall sell or lease, or offer for sale or lease (including advertising for sale or lease) or import, ship or distribute for the purposes of selling or leasing or offering for sale or lease, [a computing device prior to approval].” Furthermore, under Part 15, “operation of these devices is subject to the condition that no harmful interference is caused.”

Taken together, these sections could potentially place liability for noncompliant computing devices on the end user, a reseller, or the manufacturer of the device. In practice, liability is most often, and most harshly, assigned to the party responsible for the equipment, though it is implied for anyone connected with the product. Recently, the FCC added Rule 2.909, which defines who is considered to be the responsible party after equipment has been authorized. For certified equipment, the responsible party is the grantee; for verified equipment, the manufacturer is responsible unless the equipment is imported, in which case responsibility for continued compliance falls on the importer, or unless the reseller of the product changes the product’s name or identity, in which case the reseller is liable. Note, however, that there is an all-encompassing exception to any defense against liability: anyone who knows or has reason to know that a device fails to comply and who profits from its sale or use is liable whether or not that person is the manufacturer of the product. Therefore, while the manufacturer is generally liable for violation of the FCC rules (unless the reseller changes the product’s trade identity, in which case he or she is responsible for seeing that the device complies), the reseller can also be liable if he or she knows, or has reason to know, that the device violates the rules.

A manufacturer of a subassembly falls into a less clear-cut classification. A subassembly is not considered to be either a computer or a peripheral and is therefore not a computing device. Manufacturers of such products are treated just like parts vendors and do not have to have their subassemblies tested. Here again, however, there are two exceptions: 1) if the manufacturer knows or has reason to know that the final product is violating the FCC rules, and 2) if the manufacturer sells the subassembly to an end user and the subassembly itself connects to a computer or peripheral via a wire that is external to that device (e.g., a printed circuit card for a computer with an I/O port). In the latter instance, the manufacturer is considered not a subassembler but the manufacturer of a computing device. In the case of a company that sells plug-in boards for a computer, for example, the boards that are sold only to manufacturers that then have their products tested

do not have to be tested; however, if the company also sells those plug-in boards to end users, then the plug-in board and a typical host system must be tested in combination.

End users are not liable under the rules unless they know or have reason to know that they are violating regulations.

Finally, the engineers, salesmen, or other company employees are not liable unless they know or have reason to know that the rules are being violated. However, so-called conspiracy laws are broad in scope, and an employee who knew of a violation and did nothing about it could be held liable.