



Building The Wireless Future™

April 9, 97

RECEIVED

APR - 9 1997

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF SECRETARY

CTIA

Cellular  
Telecommunications  
Industry Association  
1250 Connecticut  
Avenue, N.W.  
Suite 200  
Washington, D.C. 20036  
202-785-0081 Telephone  
202-785-0721 Fax

Mr. William F. Caton, Secretary  
Federal Communications Commission  
1919 M Street, N.W., Room 222  
Washington, D.C. 20554

Ex Parte Contact:

CC Docket No. 92-115  
Revision of Part 22 of the Commission's Rules Governing the  
Public Mobile Services

Dear Mr. Caton:

On Wednesday, April 9, 1997, Messrs. Randall S. Coleman, Vice President for Regulatory Policy and Law, Michael F. Altschul, Vice President and General Counsel, David S. Diggs, Vice President of Operations, and Ms. Pamela A. Brewster, Deputy Director, Congressional of the Cellular Telecommunications Industry Association ("CTIA"), met with the following staff of the Commission's Wireless Telecommunications Bureau:

- Ms. Rosalind Allen, Deputy Bureau Chief
- Ms. Karen Gulick, Assistant Chief
- Ms. Jane Halprin, Legal Advisor, Commercial Wireless Division
- Mr. B.C. "Jay" Jackson, Jr., Engineering Advisor, Commercial Wireless Division

The discussion reflected CTIA's position, already on the record in the above-captioned proceeding, with an emphasis on wireless fraud. Copies of the attached documents were provided to the attending Commission staff.

Pursuant to Section 1.1206 of the Commission's Rules, an original and one copy of this letter and the attachments are being filed with your office. If there are any questions in this regard, please contact the undersigned.

Sincerely,

Jimmy L. Vaughan  
Manager for Research

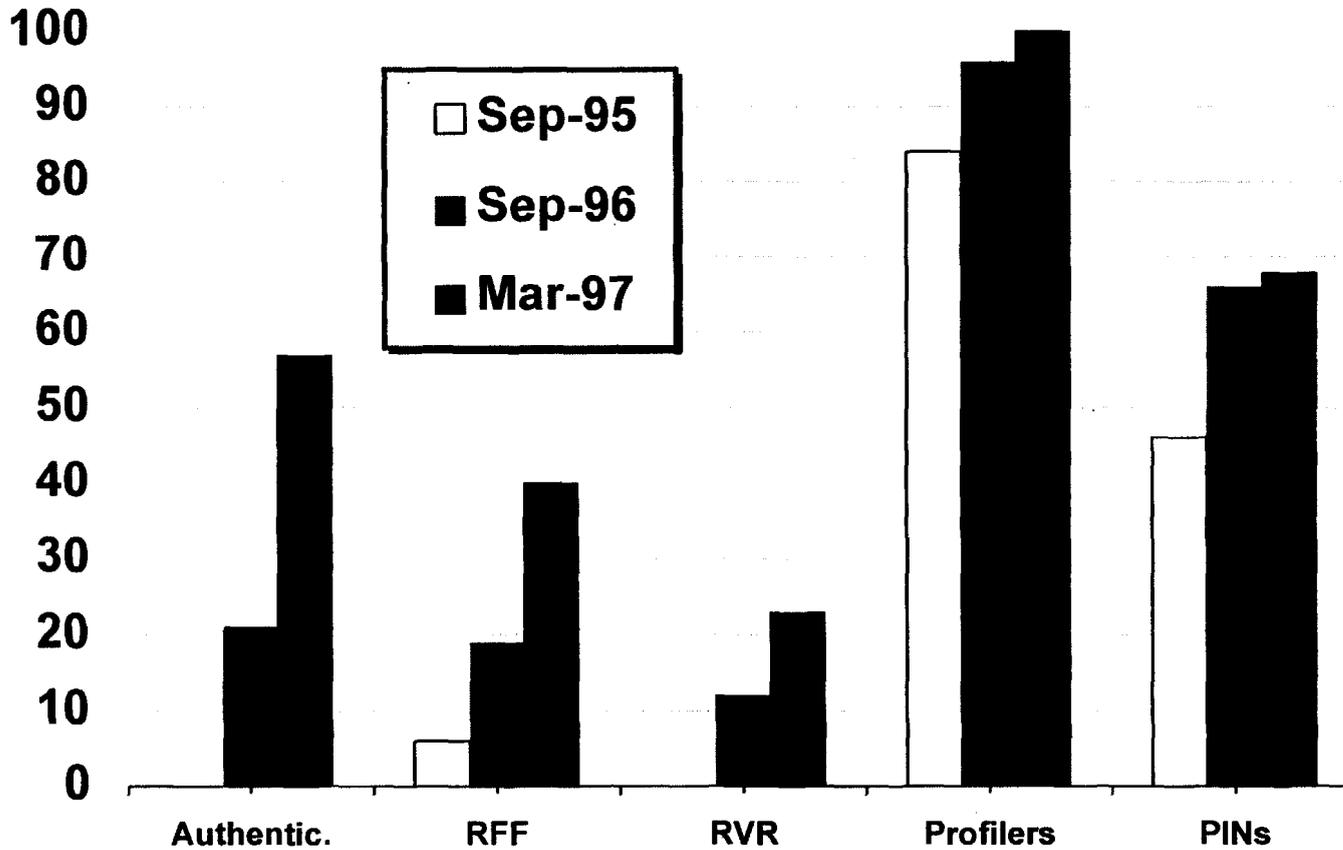
No. of Copies rec'd 04/1  
List A B C D E



# Fraud Containment: Top 50 MSAs



**A & B Systems in Top 50 Markets**



FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF SECRETARY

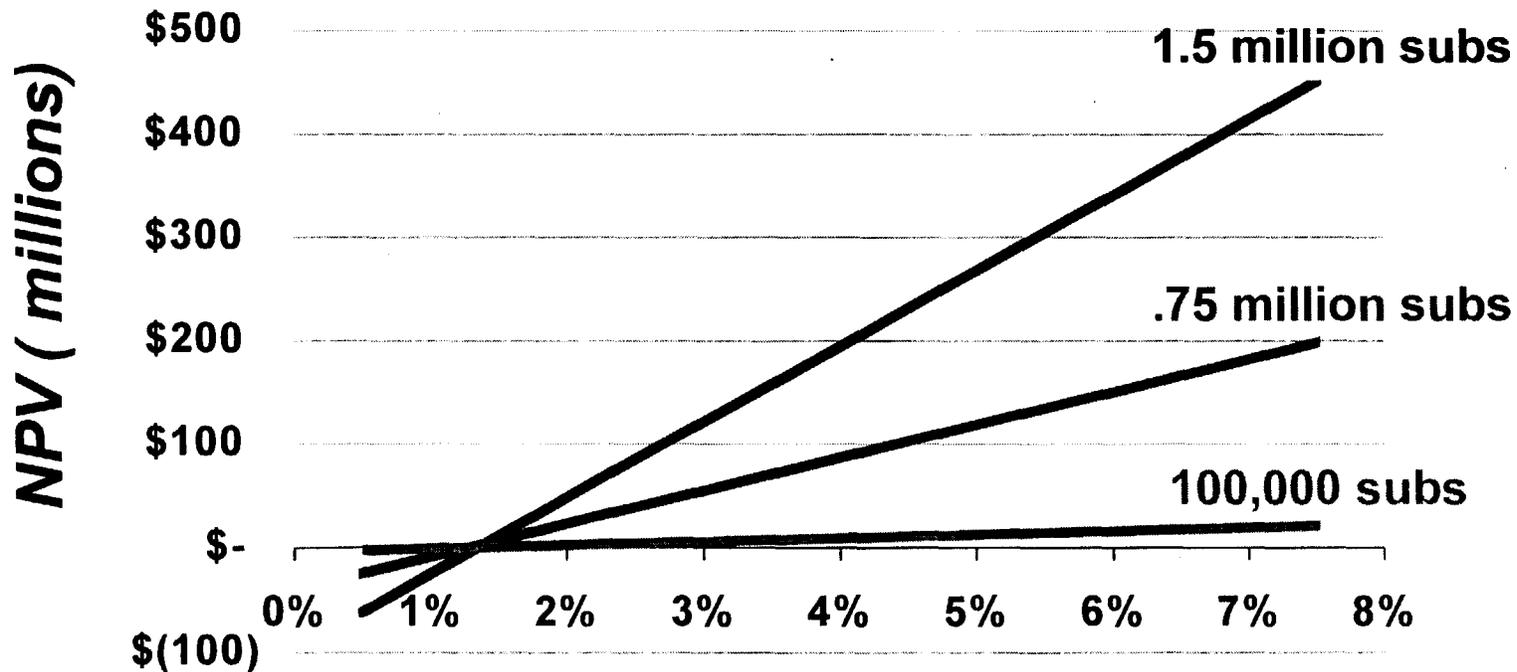
APR - 9 1997

RECEIVED

# Economics of Authentication



*Net Present Value of Authentication Investment versus Fraud Losses (% of Revenue) For Various Carrier Sizes*



Source: Hamilton Consultants, Feb 1997

CTIA

**TARGETED INFORMATION**

**To:** CEOs, Fraud Contacts, Public Relations Contacts, Washington  
Legislative Representatives

**From:** David Diggs

**Date:** March 19, 1997

**Cellular Encryption Questioned**

A team of commercial and academic cryptographers will announce tomorrow that it has "discovered a flaw in the privacy protection used in today's most advanced digital cellular phones." This announcement is made in conjunction with testimony planned for Thursday, March 20, before the House Judiciary Subcommittee on Courts and Intellectual Property hearing on H.R. 695, entitled "The 'Security and Freedom Through Encryption' (SAFE) Act." A complete copy of the cryptographers' release is attached.

The reported compromise involves CMEA (Cellular Message Encryption Algorithm) which secures certain signaling messages between a handset and the base station. These messages can consist of dialed digits, power level assignments, channel assignments or alphanumeric pages in a SMS (Short Message Service) environment.

It is important to distinguish *encryption* from *authentication*. As its name suggests, the Cellular Authentication and Voice Encryption (CAVE) protocols address both issues. The compromise claimed by this group is only loosely related to the authentication process. Authentication itself remains secure, and continues to be the industry's most effective tool to prevent cloning losses. This particular attack on CMEA, if successful, means only that a sufficiently sophisticated eavesdropper can, with considerable effort, intercept the dialed digits or short messages of a single phone, thus breaching the user's privacy.

TIA's Ad Hoc Authentication Group (AHAG) and CTIA's Fraud Technical Advisory Group (FTAG) have for some time been aware of the weaknesses of some of the ancillary protocols that make up the suite of encryption tools defined for wireless systems, and has already begun work to strengthen these ancillary protocols.

For more information contact David Diggs (202-736-3205) or Rick Kemper (202-736-3225).



Building The  
Wireless Future™

**CTIA**

Cellular  
Telecommunications  
Industry Association  
1250 Connecticut  
Avenue, N.W.  
Suite 200  
Washington, D.C. 20036  
202-785-0081 Telephone  
202-785-0721 Fax

To: Rick Kemper  
From: Bruce Schneier <schneier@counterpane.com>  
Subject: FLAW IN CELL PHONE ENCRYPTION IDENTIFIED; DESIGN PROCESS BLAMED  
Cc:  
Bcc:  
X-Attachments:

---

**CONTACTS:**

<b>Bruce Schneier</b> Counterpane Systems 612 823-1098 (voice) 612 823-1590 (fax) scnheier@counterpane.com (email)	<b>Robert Sanders, PR</b> University of California, Berkeley 510-643-6998 (voice) 510-643-7461 (fax) rls@pio.urel.berkeley.edu (email)
--	--

<b>David Wagner</b> University of California, Berkeley 510-643-9435 (voice) 510-642-5775 (fax) daw@cs.berkeley.edu (email)	<b>Lori Sinton</b> Jump Start Communications 415-938-2234 (voice) 415-938-2237 (fax) lsinton@aol.com (email)
--	--

**FLAW IN CELL PHONE ENCRYPTION IDENTIFIED; DESIGN PROCESS BLAMED**  
Telecommunications Industry Association algorithm for digital  
telephones fails under simple cryptanalysis

**MINNEAPOLIS, MN. AND BERKELEY, CA., March 20, 1997** - Counterpane Systems and UC Berkeley jointly announced today that researchers have discovered a flaw in the privacy protection used in today's most advanced digital cellular phones. This discovery points to serious problems in the closed-door process used to develop these privacy measurers. This announcement is a setback to the US cellular telephone industry, said Bruce Schneier of Counterpane Systems, a Minneapolis, MN consulting firm specializing in cryptography. The attack can be carried out in a few minutes on a conventional personal computer.

Schneier and John Kelsey of Counterpane Systems, along with graduate student David Wagner of the University of California at Berkeley, plan to publish their analysis in a paper entitled "Cryptanalysis of the Cellular Message Encryption Algorithm (CMEA)." Legislators are scheduled to hold hearings today on Rep. Goodlatte's "SAFE" (Security And Freedom Through Encryption) bill, HR695.

The problem affects numbers dialed on the key pad of a cellular handset, including any telephone, PIN, or credit cards numbers dialed. The system was supposed to protect the privacy of those dialed digits, but the encryption is weak enough that those digits are accessible to eavesdroppers with a digital scanner.

The cryptographers blame the closed-door design process and excessive pressure from U.S. military interests for problems with the privacy standard. The cellular industry attempted to balance national security with consumer privacy concerns. In an attempt to eliminate recurring security problems, the cellular standards arm of the Telecommunications Industry Association (TIA) privately designed this new framework for protecting cellular phones. The system uses encryption to prevent fraud, scramble voice communications, and protect users' privacy. These new protections are being deployed in today's digital cell phones, including CDMA, NAMPS, and TDMA.

**Not a new problem**

As early as 1992, others - including noted security expert Whitfield Diffie - pointed out fatal flaws in the new standard's voice privacy feature. The two flaws provide a crucial lesson for policy makers and consumers, the researchers said. These weaknesses are symptomatic of broad underlying problems in the design process, according to Wagner.

Many have criticized the National Security Agency (the U.S. military intelligence agency in charge of electronically monitoring foreign powers) for insinuating itself into the design process, pressuring designers to cripple the security of the cellular encryption technique and hamstringing emerging cellular security technology. "The result is weaker protection for everybody," Kelsey said.

"This is another illustration of how U.S. government efforts to control cryptography threaten the security and privacy of Americans," said David Banisar, attorney for the Electronic Privacy Information Center in Washington, D.C.

This is not the first report of security flaws in cellular telephony. Today, most cellular phone calls can be intercepted by anyone in the area listening to a scanner, as House Speaker Newt Gingrich learned this past January when someone with a scanner recorded one of his cellular calls. According to FCC estimates, the cellular telephony industry lost more that \$400 million to fraud and security problems last year.

#### **CMEA Technology**

CMEA is a symmetric cipher, like the Digital Encryption Standard (DES). It uses a 64-bit key, but weaknesses in the algorithm reduce the key to an effective length of 24 or 32 bits, significantly shorter than even the weak keys the U.S. government allows for export.

Greg Rose, program chair of the 1996 USENIX Security Symposium, put the results in context: "This break does not weaken the digital cellular fraud protections. And it's still true that digital cellular systems are much harder to casually eavesdrop on than analog phones. But it's clear from this break that a determined criminal with technical resources can intercept these systems."

Counterpane Systems is a Minneapolis, MN-based consulting firm specializing in cryptography and computer security. Bruce Schneier is president of Counterpane and author of three books on cryptography and security. David Wagner is a founding member of the ISAAC computer security research group at UC Berkeley. In the Fall of 1995, the ISAAC group made headlines by revealing a major flaw in Netscape's web browser. The authors also hasten to thank Greg Rose for his advice.

- 30 -

**For Immediate Release:  
March 20, 1997{PRIVATE }**



***Building the  
Wireless Future™***

**CTIA**

**News Media Relations**  
1250 Connecticut Ave. NW  
Washington, D.C. 20036  
202-785-0081 Main Phone  
202-736-3203 Direct  
202-467-6990 Fax

**NEWS ADVISORY:**

**ENCRYPTION OF DIGITAL  
WIRELESS PHONES**

WASHINGTON -- Today, a group of professional and academic cryptographers will announce that it has "discovered a flaw in the privacy protection used in today's most advanced digital cellular phones." Following is a set of questions and answers that arise from that announcement.

**Q. Does this mean that eavesdroppers can listen in on my phone calls?**

A. No. The encryption discussed by the researchers involves the algorithm used to encrypt numbers punched on the keypad of a phone, not the algorithm used to encrypt voice transmissions.

**Q. Is it easy to break this keypad number code?**

A. Not at this time. It involves very sophisticated cryptological knowledge. The digital encryption system now in use is designed to inhibit interception by the unsophisticated. Any technology developed by one person can be broken by another with the application of sufficient technology. This announced attack requires multiple minutes--up to hours--of high speed computer processing to break a coded message.

**Q. What is the impact of this announcement on people who now use wireless phones?**

A. Virtually none. Approximately 95 percent of the wireless phones now being used are analog phones, not digital phones. The possible impact of this announcement is only relevant to some digital phones that are now being introduced to the market.

**Q. Why didn't the wireless phone industry develop phones that have unbreakable security?**

A. Standards for phone technology are developed within the confines of federal regulations and the realities of the market place. Wireless phones are a consumer product, not a "spy v. spy" technology adequate for national security. Such a unit would have cost, battery life and call set-up times which would make it unacceptable to consumers.

**Q. Does this announcement have any impact on the industry's efforts to stop phone cloning?**

A. No. During the past year, the industry has been very successful in introducing new technologies that prevent phone cloning. These authentication and "fingerprinting" technologies operate differently and are not compromised by the cryptography announced today.

**Q. What is the industry doing about this problem?**

A. Tom Wheeler, the president and CEO of CTIA, testified before Congress on February 5, about the need to strengthen the laws protecting the security of wireless phone calls. It is currently illegal to intentionally intercept a wireless phone call. Unfortunately, whereas federal law prohibits the sale and manufacture of devices designed to eavesdrop on wireless calls, it does not extend the prohibition to cordless phones and the newer digital wireless frequencies. In regard to today's announcement, Wheeler said, "This is the horse nudging at the barn door and it is time to act before the horse is gone completely."

For more information, please contact Tim Ayers at 202-736-3203 or Jeffrey Nelson at 202-736-3207.

EDITOR'S NOTE: The cryptography researchers are Bruce Schneier, Counterpane Systems (612-823-1098); Robert Sanders, University of California, Berkeley (510-643-6998); David Wagner, University of California, Berkeley (510-643-9435); and Lori Sinton, Jump Start Communications (415-938-2234).

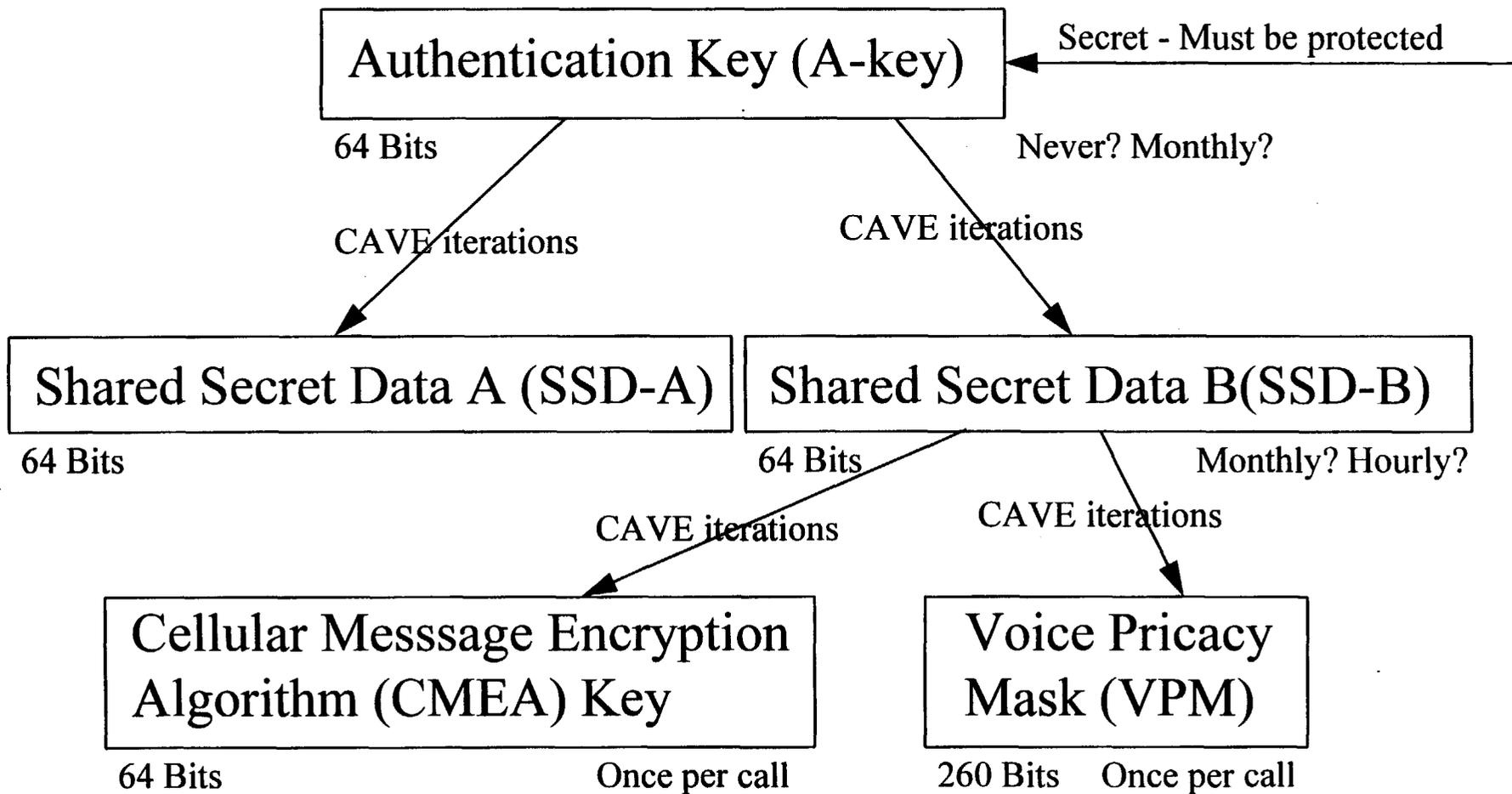
*CTIA is the international association for the wireless telecommunication industry. It represents more PCS and cellular carriers than any other association in the world.*

####

**INTERNET USERS:** News about the wireless telecommunications industry is updated several times each day on CTIA's World Wide Web site (<http://www.wow-com.com>). CTIA news releases and other information also are available on WOW-COM.

# Cellular Cryptographic Key Hierarchy

- Adapted from Les Owens, GTE Labs



Before the  
**FEDERAL COMMUNICATIONS COMMISSION**  
 Washington, DC 20554

In the Matter of	)	
	)	
Revision of Part 22 of the Commission's Rules Governing the Public Mobile Services	)	CC Docket No. 92-115
	)	
Amendment of Part 22 of the Commission's Rules to Delete Section 22.119 and Permit the Concurrent Use of Transmitters in Common Carrier and Non-common Carrier Service	)	CC Docket No. 94-46 RM 8367
	)	
Amendment of Part 22 of the Commission's Rules Pertaining to Power Limits for Paging Stations Operating in the 931 MHz Band in the Public Land Mobile Service	)	CC Docket No. 93-116
	)	

**Report and Order**

**Adopted:** August 2, 1994;

**Released:** September 9, 1994

By the Commission:

### Cellular Electronic Serial Numbers

54. **Proposal.** We proposed in the Notice a new rule (Section 22.919) intended to help reduce the fraudulent use of cellular equipment caused by tampering with the unique Electronic Serial Numbers (ESN) that identify mobile equipment to cellular systems. The purposes of the ESN in a cellular telephone are similar to the Vehicle Identification Numbers in automobiles. That is, it uniquely identifies the equipment in order to assist in recovery if it is stolen. More importantly, in the case of cellular telephones, the ESN enables the carriers to bill properly for calls made from the telephone. Any alteration of the ESN renders it useless for this purpose. The proposed rule explicitly establishes anti-fraud design specifications that require, among other things, that the ESN must be programmed into the equipment at the factory and must not be alterable, removable, or in any way able to be manipulated in the field. In addition, the proposed rules require that the ESN component be permanently attached to a main circuit board of the mobile transmitter and that the integrity of the unit's operating software not be alterable.

55. **Comments.** The commenters generally support our proposal,<sup>94</sup> but they suggest some modifications. For example, BellSouth, Southwestern Bell, GTE, and CTIA suggest that our proposal should be modified to provide that equipment already manufactured is exempt from the rule.<sup>95</sup> They argue that subjecting existing phones to this rule would be very expensive and difficult, if not impossible, to implement. Therefore, they recommend that the rule apply only

---

92 See discussion of new § 22.719 in Appendix A.

93 See discussion of new §§ 22.567 and 22.759 in Appendix A.

94 See, e.g., PacTel Comments at 2; CTIA Comments at 7-8.

95 BellSouth Comments at Appendix 2, p.36; Southwestern Bell Comments at 28-29; GTE Comments at 30; CTIA Comments at 8.

to phones manufactured after a particular date.<sup>96</sup> NYNEX recommends that we not require the ESN chip to be secured to the main circuit board of the mobile transmitter as proposed. Rather, NYNEX suggests that the ESN chip be attached to the frame of the radio and attached to the logic board by cable.<sup>97</sup> In addition, it recommends that operating software be encoded or scattered over different memory chips.<sup>98</sup> Motorola, Inc. (Motorola) and Ericsson Corp. (Ericsson), two manufacturers of cellular mobile equipment, suggest that the proposal be modified to allow authorized service centers or representatives to make necessary and required changes to ESNs in mobile and portable units in the field.<sup>99</sup>

56. Southwestern Bell recommends that the rule also apply to mobile equipment associated with a wireless private branch exchange (PBX).<sup>100</sup> CTIA suggests that the proposal be modified in several respects. First, it states that we should clarify that requiring a mobile transmitter to have a "unique" ESN, means that any particular ESN will not exist in more than one mobile unit. Second, CTIA suggests that ESN manipulation not be permitted "outside a manufacturer's authorized facility." Third, it requests that cellular mobile units be required to be designed to comply with the "applicable industry standard for authentication."<sup>101</sup> New Vector supports the proposed rule, but emphasizes that the ESN criteria should be incorporated into the type-acceptance rules to clarify that manufacturers will be subject to the Commission's enforcement procedures if they do not comply with the ESN requirements.<sup>102</sup>

57. C2+ Technology (C2+) requests that we allow companies to market ancillary cellular equipment that emulates ESNs for the purpose of allowing more than one cellular phone to have the same telephone number. It argues that emulating ESNs in the way it describes benefits the public, does not involve fraud, and retains the security and integrity of the cellular phones.<sup>103</sup> In opposition, Ericsson asserts that the rules should include procedures to ensure that ESNs are not

---

96 For example, BellSouth suggests that the anti-fraud measures should not apply to equipment type-accepted before January 1, 1993.

97 NYNEX Comments at 8.

98 Id. at 8-9.

99 Ericsson Reply Comments at 2-5; Motorola Reply Comments at 3.

100 Southwestern Bell Comments at 29.

101 CTIA Comments at 8.

102 New Vector Comments at Appendix I, p.44.

103 C2+ Comments at 1-2.

easily transferable through the use of an encrypted data transfer device.<sup>104</sup> Similarly, New Par suggests that the proposed rule proscribe activity that does not physically alter the chip yet affects the radiated ESN by translating the ESN signal that the mobile unit transmits.<sup>105</sup>

58. **Discussion.** The record before us demonstrates the need for measures that will help reduce the fraudulent use of cellular equipment caused by tampering with the ESN. We therefore adopt the proposed rule for the reasons set forth below.

59. Contrary to the suggestion of one commenter, the ESN rule will not prevent a consumer from having two cellular telephones with the same telephone number. Changing the ESN emitted by a cellular telephone to be the same as that emitted by another cellular telephone does not create an "extension" cellular telephone. Rather, it merely makes it impossible for the cellular system to distinguish between the two telephones. We note that Commission rules do not prohibit assignment of the same telephone number to two or more cellular telephones.<sup>106</sup> It is technically possible to have the same telephone number for two or more cellular telephones, each having a unique ESN.<sup>107</sup> If a cellular carrier wishes to provide this service, it may. In this connection, we will not require that use of cellular telephones comply with an industry authentication procedure as requested by CTIA, as this could have the unintended effect of precluding multiple cellular telephones (each with a unique ESN) from having the same telephone number.

60. Further, we conclude that the practice of altering cellular phones to "emulate" ESNs without receiving the permission of the relevant cellular licensee should not be allowed because (1) simultaneous use of cellular telephones fraudulently emitting the same ESN without the licensee's permission could cause problems in some cellular systems such as erroneous tracking or billing; (2) fraudulent use of such phones without the licensee's permission could deprive cellular carriers of monthly per telephone revenues to which they are entitled; and (3) such altered phones not authorized by the carrier, would therefore not fall within the licensee's blanket license, and thus would be unlicensed transmitters in violation of Section 301 of the Act. Therefore, we agree with New Par and Ericsson that the ESN rule should proscribe activity that

---

104 Ericsson Reply Comments at 3-4.

105 New Par Comments at 21-22.

106 The telephone number is referred to in the cellular compatibility specification as the Mobile Identification Number or "MIN".

107 It is not technically necessary to have the same ESN in order to have the same telephone number. Nevertheless, the authentication software used by some cellular systems does not permit two cellular telephones with the same telephone number. In such cases, cellular carriers should explain to consumers who request this service that their system is not yet capable of providing it.

does not physically alter the ESN, but affects the radiated ESN, including activities that transfer ESNs through the use of an encrypted data transfer device.

61. With respect to the proposal to allow alteration of ESNs by manufacturers' authorized service centers or representatives, we note that computer software to change ESNs, which is intended to be used only by authorized service personnel, might become available to unauthorized persons through privately operated computer "bulletin boards". We have no knowledge that it is now possible to prevent unauthorized use of such software for fraudulent purposes. Accordingly, we decline to make the exception requested by Motorola and Ericsson.

62. We further agree with the commenters that it would be impractical to apply the new rule to existing equipment. Accordingly, we are not requiring that cellular equipment that is currently in use or has received a grant of type-acceptance be modified or retrofitted to comply with the requirements of this rule. Thus, the ESN rule will apply only to cellular equipment for which initial type-acceptance is sought after the date that our rules become effective. Nevertheless, with regard to existing equipment, we conclude that cellular telephones with altered ESNs do not comply with the cellular system compatibility specification<sup>108</sup> and thus may not be considered authorized equipment under the original type acceptance. Accordingly, a consumer's knowing use of such altered equipment would violate our rules. We further believe that any individual or company that knowingly alters cellular telephones to cause them to transmit an ESN other than the one originally installed by the manufacturer is aiding in the violation of our rules. Thus, we advise all cellular licensees and subscribers that the use of the C2+ altered cellular telephones constitutes a violation of the Act and our rules.

63. With respect to NYNEX's proposed modifications for securing the ESN chip to the mobile transmitter, the record does not convince us that these modifications will make the ESN rule more effective. Therefore, we do not adopt NYNEX's proposal. We agree with Southwestern Bell that the ESN rule should apply to mobile equipment associated with wireless PBX if the equipment can also be used on cellular systems. We also clarify that the new ESN rule prohibits the installation of an ESN in more than one mobile transmitter. Finally, as suggested by New Vector, we amend the type-acceptance rule to refer to the newly adopted ESN rule.<sup>109</sup>

#### **Use of Part 22 Transmitters in Non-Common Carrier Services**

64. **Proposal.** Section 22.119 of the Rules currently prohibits the concurrent licensing and use of transmitters authorized to provide common carrier service under Part 22 of the Rules

---

108 See old § 22.915, which becomes new § 22.933 in Appendices A and B.

109 See discussion of new § 22.377 in Appendix A.

this paragraph in lieu of compliance with paragraph (b) of this section and the audio filter requirement of § 22.915.

(1) The mean power of any emission removed from the carrier frequency by a displacement frequency ( $f_d$  in kHz) must be attenuated below the mean power of the unmodulated carrier ( $P$ ) as follows:

(i) On any frequency removed from the carrier frequency by more than 12 kHz but not more than 20 kHz:

at least  $117 \log(f_d - 12)$  dB;

(ii) On any frequency removed from the carrier frequency by more than 20 kHz, up to the first multiple of the carrier frequency:

at least  $100 \log(f_d + 11)$  dB or 60 dB or  $43 + 10 \log P$  dB, whichever is the lesser attenuation;

(2) For mobile stations, modulating signals other than the supervisory audio tone in the frequency range of 5.9 to 6.1 kHz must be attenuated, relative to the level at 1 kHz, at least 35 dB.

(d) F1D emission mask. For F1D emissions, the mean power of emissions must be attenuated below the mean power of the unmodulated carrier ( $P$ ) as follows:

(1) On any frequency removed from the carrier frequency by more than 20 kHz but not more than 45 kHz:

at least 26 dB;

(2) On any frequency removed from the carrier frequency by more than 45 kHz but not more than 90 kHz:

at least 45 dB;

(3) On any frequency removed from the carrier frequency by more than 90 kHz, up to the first multiple of the carrier frequency:

at least 60 dB or  $43 + 10 \log P$  dB, whichever is the lesser attenuation.

(e) Out of band emissions. The mean power of emissions must be attenuated below the mean power of the unmodulated carrier ( $P$ ) on any frequency twice or more than twice the fundamental frequency by:

at least  $43 + 10 \log P$  dB.

(f) Mobile emissions in base frequency range. The mean power of any emissions appearing in the base station frequency range from cellular mobile transmitters operated must be attenuated to a level not to exceed -80 dBm at the transmit antenna connector.

(g) Interference from spurious emissions. If any emission from a transmitter operating in this service results in interference to users of another radio service, the FCC may require a greater attenuation of that emission than specified in this section.

(h) Measurement procedure. The following spectrum analyzer bandwidth settings should be used for measurement of spurious emissions:

(1) When operating in the radiotelephony mode or the supervisory

audio tone mode:

(i) For any emission not more than 45 kHz removed from the carrier frequency: 300 Hz;

(ii) For any emission more than 45 kHz removed from the carrier frequency: 30 kHz.

(2) When operating in the wideband data mode or the signaling tone mode:

(i) For any emission not more than 60 kHz removed from the carrier frequency: 300 Hz;

(ii) For any emission more than 60 kHz removed from the carrier frequency: 30 kHz.

#### § 22.919 Electronic serial numbers.

The Electronic Serial Number (ESN) is a 32 bit binary number that uniquely identifies a cellular mobile transmitter to any cellular system.

(a) Each mobile transmitter in service must have a unique ESN.

(b) The ESN host component must be permanently attached to a main circuit board of the mobile transmitter and the integrity of the unit's operating software must not be alterable. The ESN must be isolated from fraudulent contact and tampering. If the ESN host component does not contain other information, that component must not be removable, and its electrical connections must not be accessible. If the ESN host component contains other information, the ESN must be encoded using one or more of the following techniques:

(1) Multiplication or division by a polynomial;

(2) Cyclic coding;

(3) The spreading of ESN bits over various non-sequential memory locations.

(c) The ESN must be factory set and must not be alterable, transferable, removable or otherwise able to be manipulated. Cellular mobile equipment must be designed such that any attempt to remove, tamper with, or change the ESN chip, its logic system, or firmware originally programmed by the manufacturer will render the mobile transmitter inoperative.

#### § 22.923 Cellular system configuration.

Mobile stations communicate with and through base transmitters only. Base transmitters communicate with mobile stations directly or through cellular repeaters. Auxiliary test stations may communicate with base or mobile stations for the purpose of testing equipment.

#### § 22.925 Prohibition on airborne operation of cellular telephones.

Cellular telephones installed in or carried aboard airplanes, balloons or any other type of aircraft must not be operated while such aircraft are airborne (not touching the ground). When any aircraft leaves the ground, all cellular telephones on board that aircraft must be turned off. The following notice must be posted on

RECEIVED

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF GEORGIA  
BRUNSWICK DIVISION

PALMER WIRELESS, INC., )  
d/b/a CELLULAR ONE, and )  
GEORGIA R.S.A. #12 PARTNERSHIP, )  
) )  
Plaintiffs, )  
) )  
v. ) )  
) )  
FRANCES E. ("BUNNY") MARSHALL, )  
and MARSHLAND COMMUNICATIONS, )  
INC., )  
) )  
Defendants. )

CASE NUMBER CV295-201

OPINION AND ORDER

Plaintiffs, Palmer Wireless, Inc., d/b/a CELLULAR ONE (hereinafter, "Cellular One"), and GEORGIA R.S.A. #12 PARTNERSHIP (hereinafter, "Alltel") filed their Complaint against Frances E. ("Bunny") Marshall and Marshland Communications, Inc., on December 6, 1995, requesting, among other relief, a temporary restraining order, preliminary injunction, and permanent injunction. The hearing on the temporary restraining order, scheduled for Tuesday, December 19, 1995, was cancelled and a final hearing for purposes of FRCP 65 was held on Thursday, December 28, 1995. Both parties having briefed the Court and had the opportunity to present evidence, the Court finds as follows:

## FACTS

Each cellular phone is manufactured with a unique electronic serial number (ESN) that, by law, is factory set at the time of manufacture. The ESN is a 32-bit binary number that identifies the cellular phone much like an automobile's vehicle identification number or VIN uniquely identifies a car. The ESN is central to the integrity of the cellular operating system, identifying the particular phone to ensure that access to the system is authorized and to track usage for billing purposes.

In addition to the ESN, a mobile identification number (MIN) or phone number is assigned by the local carrier when the cellular phone is activated for service. Once the MIN is assigned and service activated, the ESN/MIN combination is entered into the carrier's mobile telephone switching office (MTSO). The MTSO is connected to a honeycomb of cell sites or fixed transmitting and receiving stations that act as the airwaves relay for voice communications and allows the carrier to bill for services.

When a cellular phone is turned on, even though no call is being made or received, the phone's ESN/MIN combination automatically is transmitted at regular intervals to the nearest "cell site." This continuous exchange of ESN/MIN signaling information between each phone and a cell site is known as "autonomous registration" and allows a subscriber to be tracked so that incoming calls can be received and outgoing calls can be made over the network. Thus, as a subscriber moves through a service area, the phone seeks out the nearest cell site and

the strongest signal, letting the network know that the phone is available to receive and send calls.

When a subscriber actually makes or receives a call, the signal becomes continuous for the duration of the call. The signal literally gets "handed off" seamlessly to the next cell site as the mobile user travels through the area.

Because the ESN/MIN combination is continuously transmitted in the clear across the network, it may be unlawfully scanned by criminals who set up road-side stations to acquire the signals and then reprogram or "clone" cellular phones with the stolen ESN/MIN combinations to emulate the authorized phone. In essence, these road-side thieves steal the access keys to the operating system. The theft may go undetected until a subscriber receives a bill for the unauthorized service (which the carrier ultimately absorbs) or until the system identifies the cloning when both phones are used simultaneously. In both cases, the carrier's system is seriously degraded and administrative costs are incurred in the investigation of the fraud, termination of the service, and reactivation of new service for the subscriber.

Store-front emulation services, such as those engaged in by Marshland, have sprung up across the country. Rather than steal the ESNs over the airwaves, emulators persuade subscribers to purchase so-called "extension" phone services, which is nothing more than the cloning of their authorized phone. A cloned extension phone has the same impact on the cellular system as any other fraudulent phone and may result in termination of a subscriber's service, particularly if both phones are used at the same time in the same service area.

Plaintiffs are licensed by the Federal Communications Commission ("FCC") to provide cellular communications services on their authorized frequencies in the Brunswick area, including the counties of Camden, Glynn, Liberty, Long, McIntosh, and Wayne. Plaintiffs each contract with their subscribers that only one telephone number will be assigned to one cellular phone. Cellular One's contract also provides that the subscriber will ensure that his or her cellular phone complies with FCC Rules and Regulations.

Frances E. Marshall (hereinafter, "Marshall") is an officer of, and founded, Marshland Communications, Inc. (hereinafter "Marshland"). Marshland is a Georgia corporation with its principal place of business on St. Simons Island, Georgia. Neither Defendant is licensed by the FCC to operate a cellular telephone network. The exclusive activity of Defendants Marshall and Marshland is to solicit customers, in the area in which Plaintiffs are licensed by the FCC, for the express purpose of removing a cellular telephone's factory assigned and installed ESN and replacing same with the ESN assigned to another cellular telephone that has been activated for use on one of the Plaintiffs' cellular networks. The cellular telephone, with the altered ESN, is programmed by Defendants with the MIN assigned to a cellular subscriber. The cloned cellular telephone then emulates a cellular telephone authorized for use on one of the Plaintiffs' cellular networks. In exchange for this emulation service, Defendants charge a fee of around \$180. Defendants have cloned the cellular telephones of a substantial number of subscribers to the cellular telephone services of Plaintiffs. Defendants do not notify the carrier when they clone a subscriber's phone, nor do they verify with the carrier that the subscriber has an active account.

As will later be shown in this Order, Defendants' actions are illegal, and Plaintiffs have been damaged by same. First, emulation or cloning enables one cellular phone to emulate another cellular phone, enabling a customer to use more than one telephone for the same telephone number and thereby avoiding monthly access charges charged by Plaintiffs and other cellular licensees for each phone. This results in a loss of revenue to Plaintiffs and may result in higher monthly access fees for authorized users of Plaintiffs cellular networks.

Second, cloning of ESNs by Defendants produce cellular phones which do not conform to the FCC specifications in 47 C.F.R. § 22.933. Plaintiffs hold a blanket license from the FCC to operate a cellular system in the Brunswick area. Plaintiffs are only authorized to operate that system in combination with individual cellular phones that meet the FCC's technical requirements, including its rules that each of those transmitters have its own unique ESN. 47 C.F.R. § 22.927 charges Plaintiffs with the responsibility of exercising effective operational control over mobile stations receiving service through its cellular systems. On each occasion that Defendants place an unauthorized transmitter in service on Plaintiffs' systems, they are causing the violation of the terms of FCC licenses. (See, Second ESN Order, ¶ 60).

Third, the contract between Plaintiffs and their subscribers provide that the subscribers will only have one telephone number per phone and that the subscribers will not violate FCC regulations. The emulation services provided by Defendants cause Plaintiffs' subscribers to violate their contract with Plaintiffs.

Fourth, three channels are necessary to operate a cellular phone. When two cellular phones, one of which emulates the other, are operating in different cell sites, both

phones will ring when that cellular phone number is dialed. This ties up six channels thereby using double the normal capacity from one of the Plaintiffs' networks and depriving others of access if the cellular network is at its maximum capacity. A fifth problem is that, when one of the cellular phones is answered, the network terminates the call to the other cellular phone. The cellular network cannot determine which telephone an individual is attempting to call when one of them has been cloned. A charge for the telephone call is billed to the subscriber whose phone has been answered, even if the caller was attempting to reach the individual possessing the other cellular phone with the same ESN and MIN. A second phone call would then be necessary to attempt to reach the intended cellular phone. This results in two charges to the subscriber when only one should have been necessary.

Finally, Plaintiffs operate an administrative review of subscribers for purposes of finding fraud. Same consists of a computerized system which reviews usage patterns and profiles. Any spike in usage for one cellular phone is investigated. Other indicia of fraud include using a cellular phone to reach a foreign country and staying on-line for more than ten or fifteen minutes. Having a number of emulated or cloned phones operating off the same subscriber account creates a spike in usage which then ties up resources for purposes of an investigation. The cellular network operator, such as the Plaintiffs, cannot differentiate between those who are "free riding," i.e., stealing ESNs and MINs randomly from the air and then using same to gain access to a cellular network, and those who are cloning, like Defendants.

LAW

Part I

FCC Orders

Via 46 USC §151, the Federal Communications Commission (FCC) was given plenary authority to regulate the airways. §301 provides for the regulation of radio communications and provides the authority of the FCC to require licenses of radio frequency energy. Thus, a person or entity needs a license from the FCC to use the airwaves. The FCC licenses two cellular carriers in each market to provide cellular services.

47 CFR §22.901 states that carriers must provide service to all customers in the area and provides that carriers can terminate any subscriber who does not comply with the carrier's duties under 47 CFR §22.927. 47 CFR §22.927 provides that the cellular carrier has authorization extending to each mobile unit in its network. Since the inception of cellular networks and FCC regulation of same, the FCC has required one ESN per telephone.

On May 4, 1981, the FCC released an Order entitled "An Inquiry Into the Use of the Bands 825-845 MHz and 870-890 MHz for Cellular Communications Systems; and Amendment of Parts 2 and 22 of the Commission's Rules Relative to Cellular Communications Systems," 86 F.C.C.2d 469 (1981) in which it, among other things, adopted technical specifications for the use of cellular telephones, including a requirement that each phone have a unique ESN. See 86 F.C.C.2d at 508 and n. 78,573, and 593. Originally, this requirement was found at Section 2.3.2 of the FCC's Mobile Station-Land Station Compatibility

Specifications (Office of Engineering and Technology Bulletin No. 53) incorporated in FCC Rule 22.915 (now 47 C.F.R. § 22.933). The May 4, 1981 FCC Order (the "First ESN Order") was published in the Federal Register on May 21, 1981 (46 Fed. Reg. 27655) with corrections on June 16, 1981 (46 Fed. Reg. 31417). The FCC adopted this rule "in accordance with its legislatively delegated rulemaking authority . . . [which is] binding on all applicable persons." *South Central Bell Telephone Co. v. Louisiana Public Service Comm.*, 744 F.2d 1101, 1115 (5th Cir. 1985).

On October 2, 1991, the FCC issued Public Notice (20011), Report No: CL-92-3 entitled "CHANGING ELECTRONIC SERIAL NUMBERS ON CELLULAR PHONES IS A VIOLATION OF THE COMMISSION'S RULES." It states, in pertinent part, that:

Phones with altered ESN's do not comply with the Commission's rules and any individual or company operating such phones or performing such alterations is in violation of Section 22.915 of the Commission's rules and could be subject to appropriate enforcement action. (Emphasis supplied.)

In response to an FCC Notice of Proposed Rule Making, released June 12, 1992, 7 F.C.C. Rcd. 3658, which was published in the Federal Register on July 1, 1992 (57 Fed. Reg. 29260), C2+ Technology, a company that altered ESNs, requested the FCC to amend the Commission's rules and allow companies to market ancillary cellular equipment that emulates ESNs for the purpose of allowing more than one cellular telephone to have the same telephone number. See paragraph 57 of the Second ESN Order, 76 RR2d 1 at 15.

The FCC specifically rejected the proposed amendment of the emulator. The Commission wrote:

Further, we conclude that the practice of altering cellular phones to "emulate" ESNs without receiving the permission of the relevant cellular licensee should not be allowed because (1) simultaneous use of cellular telephones fraudulently emitting the same ESN without the licensee's permission could cause problems in some cellular systems such as erroneous tracking or billing; (2) fraudulent use of such phones without the licensee's permission could deprive cellular carriers of monthly per telephone revenues to which they are entitled; and (3) such altered phones not authorized by the carrier would therefore not fall within the licensee's blanket license, and thus would be unlicensed transmitters in violation of Section 301 of the Act.

See paragraph 60 of the Second ESN Order, 76 RR2d 1 at p. 15.

The Commission further concluded:

. . . Nevertheless, with regard to existing equipment, we conclude that cellular telephones with altered ESNs do not comply with the cellular system compatibility specification<sup>1</sup> and thus may not be considered authorized equipment under the original type acceptance. Accordingly, a consumer's knowing use of such altered equipment would violate our rules. We further believe that any individual or company that knowingly alters cellular telephones to cause them to transmit an

---

<sup>1</sup>See previous 47 CFR § 22.915, which became new 47 CFR § 22.933, adopted in the Second ESN Order.

ESN other than the one originally installed by the manufacturer is aiding in the violation of our rules. Thus, we advise all cellular licensees and subscribers that the use of the C2+ altered cellular telephones constitutes a violation of the Act and our rules. (Emphasis added)

See paragraph 62 of the Second ESN Order, 76 RR2d 1 at p. 15.

On September 9, 1994, the FCC released the above referenced Order entitled "Revision of Part 22 of the Commission Rules Governing the Public Mobile Services." This FCC Order (the "Second ESN Order") was published in its entirety in *Pike and Fischer Radio Regulations* (76 RR 2d Page 1). Summary of the same was published in the Federal Register on November 17, 1994 (59 Fed. Reg. 59502). The Second ESN Order, also known as Order No. 94-210, readopted and renumbered 47 C.F.R. § 22.915 as 47 C.F.R. § 22.933. The Second ESN Order adopted 47 C.F.R. § 22.919. These two provisions of the C.F.R. codify the First and Second ESN Orders. Section 22.919(a) requires that "[e]ach mobile transmitter in service must have a unique ESN." 47 C.F.R. § 22.933 states that:

The serial number is a 32 bit binary number that uniquely identifies a mobile station to any cellular system. It must be factory-set and not readily alterable in the field. The circuitry that provides the serial number must be isolated from fraudulent contact and tampering. Attempts to change the serial number circuitry should render the mobile station inoperative. (Office of Engineering and Technology Bulletin No. 53, Section 2.3.2).