Technical Overview - SSD Update

- Randomly scheduled by the AC, on a per mobile basis
- Requires MS to authenticate the AC, as well
- A successful "Unique Challenge" is mandatory
- Occurs on "Bearer" channels ONLY for Roamers

Technical Overview - Global Challenge

- When SSD is shared, VLR conducts the Global Challenge for Roamers
- RAND, a random number, included in the OMT (FoCC)
- AUTHR from MS = f(SSD, RAND, ESN, MIN1) on Initial registration
- AUTHR from MS = f(SSD, RAND, ESN, Dialed Digits) on Originations and Page responses

Technical Overview - Global Challenge (contd)

- AUTHR from MS must match AUTHR computed internally at the AC/VLR for authentication to be successful
- Access attempt is ignored if comparison fails, except for Emergency and Customer service calls

Unique Challenge

- Per Mobile basis, on Control and/or Bearer channels
- AUTHU from MS = f(SSD, RANDU, ESN, MIN1, MIN2)
- AUTHU from MS must match AUTHU computed by the AC/VLR
- Unique Challenge is ALSO forced, when in doubt

Considerations

- *A-key and SSD are NEVER transmitted over-the-air*
- *SSD is transmitted to the VLR over SS7 links, if SSD is shared*
- *Expected recycle rate for the Random numbers is VERY HIGH.*
- *ECP/VLR detect authentication with Default values of RAND, A-Key and SSD*

In Closing...

- *Service provisioning is complicated by A-Key distribution*
- *Response strategies to be worked out for:*
  - *Detection of compromised A-Key*
  - *Detection of compromised SSD*

In Closing... (Contd)

- *Procedures to be worked out for:*
  - *A-Key and SSD Updates*
  - *Integration with Customer service*
- *Fraud vulnerbility with Cloning continues until Auth coverage is 100%*
- *Network impact under both SSD Shared and SSD not Shared, must be evaluated*

AT&T Wireless Services, Inc.
17th Floor
32 Avenue of the Americas
New York, NY 10013
212 830-6360
FAX 212 334-1221

May 3, 1996

Michele Farquhar
Chief,
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

Re: C-Two-Plus Technology, Inc. Petition for Reconsideration
CC Docket No. 92-115

Dear Ms. Farquhar:

AT&T Wireless Services, Inc. ("AWS") hereby responds to the many submissions regarding the pending Petition for Reconsideration of C-Two-Plus Technology, Inc. ("C2+") filed with respect to the Federal Communications Commission's Report and Order, 9 FCC Rcd. 6513 (1994) ("Order"), including C2+'s most recent ex parte submission to Chairman Hundt dated February 14, 1996. A copy of this letter will also be forwarded to the Secretary of the Commission for inclusion in the administrative record in CC Docket No. 92-115.

A. THE CONDUCT OF C2+ AND ITS EXTENSION PHONE FRANCHISES HAS BEEN ANTI-CONSUMER AND IN DIRECT VIOLATION OF THE COMMISSION'S ORDER

The Commission should carefully consider the conduct of C2+ and its franchises while the Petition of C2+ for Reconsideration has been pending -- it has been nothing short of contempt, both for the Commission and the law. The Commission's Order has been in full force and effect, prohibiting C2+ and its

Recycled Paper

undisclosed franchises from emulating cellular phones. Yet, C2+ and its coterie of extension phone companies have continued to flaunt the Order across the country.[1]

AWS is aware of no authority or rule that permits a petitioner before the FCC to engage in prohibited conduct pending the outcome of reconsideration of a rule. While C2+ may argue that the Commission's anti-cloning rule is unfair because C2+ did not participate in the rule-making or that the rule is not based on record evidence, C2+ may not disregard that rule on its belief in the efficacy of these arguments. The Commission has repeatedly made clear that:

1. Knowing use of a cellular telephone with an altered ESN violates FCC rule (§ 22.377) requiring use of type accepted equipment.

2. Use of equipment that carrier has not authorized for use on its system constitutes violation of Section 301 of Communications Act of 1934, as amended (47 U.S.C. § 301).

3. Any individual or company that knowingly alters cellular telephone to cause it to transmit ESN other than the one originally installed by manufacturer is aiding in violation of FCC rules.

4. Use of C2+ altered cellular telephones constitutes a violation of the Communications Act and FCC Rules.[2]

---

[1] Not only does C2+ continue to violate the law, but they also actively misrepresent the statements of Commission staff to courts and the public. For example, in litigation between C2+ and various cellular carriers pending in federal court in Alabama, C2+ has asked the industry to admit that Steve Markendorf and John Cimko made statements to the press that C2+ was not subject to Commission jurisdiction and that its activities were not illegal. *See* Plaintiff C-Two Plus Technology, Inc.'s Modified Requests for Admission, Nos. 2, 23 & 24. These Requests, of course, mischaracterize the statements of the individuals in question as well as the position of the Commission and may result in the need for Commission staff to be available for deposition and/or trial to explain the erroneous allegations of C2+.

[2] *See* C2+ letter to Chairman Hundt dated February 14, 1996, Attachment 1 at 2 ("Agenda for July 27, 1995 Ex Parte Presentations")

Disregard for the law and the Commission's rules demonstrates that C2+'s Petition is not about providing consumer services, but rather is about its own profit at the expense of the consumer and the service provider. To illustrate the point, it is necessary to review briefly the emulator suits over the last nine months, copies of which have been provided previously to the Commission by the Cellular Telecommunications Industry Association ("CTIA").[3]

There have been at least seven cases to date permanently enjoining emulators from engaging in extension phone cloning[4] and more are pending in the courts. In those cases, the extension phone companies have argued, among other things, that (1) the FCC's Order is a mere policy statement not entitled to any weight and unenforceable as a matter of law under Section 401(b) of Title 47; (2) even if the policy statement were an enforceable order, emulation does not violate it because the

---

[3] C2+ recently has cited some of these cases to the Commission as evidence of carrier efforts to enforce the law against "small providers of cellular extension phone services." *See* C2+ letter, *supra* note 1 at 2. As noted in more detail below, these so-called "small" companies are for the most part local franchises of C2+ and other cloning service providers. They are distributors of illegal cellular phones, the profits of which C2+ readily shares and enjoys. C2+ also suggests that these "small" providers have agreed to injunctions because "they did not have the financial ability to engage in protracted litigation with carriers." *Id.* To the contrary, several of the cases cited below have been fully briefed and argued to the court, resulting in binding decisions to enjoin unlawful behavior.

[4] *See Houston Cellular Telephone Co. v Nelson*, No. 95-617 (S.D. Tex., Mar. 15, 1995); *Southwestern Bell Mobile Systems v. Cell Phone Extensions*, No. 4:95-CV-796-CAS (E.D. Mo., May 24, 1995); *Nynex Mobile Communications Co. v. Cellular Emulation Services*, No. 95 Civ. 4335 (S.D. N.Y. 1995) (Settlement); *Miss. Cellular Telephone Co. v. Cellular Extension Phone Services*, No. 1:95CV311BrR (S.D. Miss. June 13, 1995); *MCC/McCaw Cellular v. Cell Phone Extensions*, No. 3- 95-660 (D. Minn., July 19, 1995); *Alltel Mobile Communications of Arkansas v. Phone Clone and Cell Ex*, No. Lr-C-95-544 (W.D. Ark., Sept. 18, 1995); *Palmer Wireless v. Marshland Communications*, No. CV295-201 (S.D. Ga., Dec. 29, 1995); *Midwest Cellular Telephone Co. v. Meyers*, No. CIV-96-31-R (W.D. Okla., Jan. 8, 1996); and *US West NewVector Group v. Cell Phone Extensions*, No. CIV 95-1700-PHX-SMM (D. Ariz., Feb. __, 1996). *Metroplex Telephone Co. v. Ellis*, No. 3:96-CV-0449-D (N.D. Tex., Feb. 15, 1996) is pending in the Dallas Division. *CPSI v. Florida*, No. 95-13347(18) (17th Judicial Cir., Broward Cty 1996) upheld the Florida anti-cloning or emulation statute against a constitutional challenge by an admitted extension phone cloner.

Order only applies to equipment whose initial type-acceptance was sought after January 1, 1995; and (3) carriers are not injured by the conduct even if it is unlawful.

To add insult to these frivolous legal positions, the extension phone companies also have asserted that courts should not hear the carrier's injunctive relief cases at all because the Commission is "reconsidering" the rule, implying that the petition will be granted and citing Commission inaction as proof. While courts have uniformly rejected all of these spurious claims,[5] the actions of C2+ and its local franchises before the courts speak volumes about C2+'s contempt for the Commission, consumers and licensed carriers and is the shape of things to come should the Commission grant the Petition.[6]

---

[5] We do not review the responses to each of the defenses raised by C2+ companies inasmuch as carriers across the country have done so in pleadings already provided to the Commission under separate cover. Of course, the Commission itself is best situated to recognize the bald-faced attempt to mislead the courts and the public. Howard Davenport recently confirmed that the Commission viewed C2+ technology as unlawful manipulation of the ESN:

> Maintaining the integrity of the ESN is key to preventing cellular fraud on today's analog cellular systems. While it has always been the Commission's view that altering the ESN violated the rules, we proposed a new rule section that explicitly required, 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.

Remarks of Howard Davenport, Chief, Enforcement Division, Wireless Telecommunications Bureau, before the Communications Fraud Control Association, Nashville, TN, September 1995, *reprinted and summarized in* The Communicator, Nov./Dec. 1995 at 7. Yet, C2+ has not heard the Commission or worse, simply chooses to ignore it.

[6] It can only be contempt when one of the cloning companies asserts that the Commission's Order is inapplicable to his operations because his company does not "utilize equipment or software from C2+, but instead uses different technology licensed from two other independent sources." *See US West NewVector Group v. Cell Phone Extensions*, No. CIV 95-1700-PHX-SMM (D. Ariz., Feb. __, 1996), Defendant's Responses to, and Partial Cross-Motion for, Partial Summary Judgment at 10-11. C2+ emulators, like street-corner cloners, recognize the market opportunities present in an enforcement vacuum -- they multiply to fill the void and carrier and customer both suffer.

It is obvious that C2+-based companies interfere with the carrier-customer contractual relationship because subscriber service contracts generally require the use of only one cellular phone per mobile identification number ("MIN") and electronic serial number ("ESN"). More subtle than this unlawful interference with contractual relations, C2+ and its cloning companies dupe generally innocent customers into paying $250 or more for an illegal phone that the cloning companies know will be shut down when discovered by the carrier. Of course, these storefront operations are short-lived and frequently disappear as quickly as they appear, having made the quick profit from the consumer and leaving the subscriber with no recourse for the loss.

While C2+ has accused cellular carriers of being anti-competitive and anti-consumer, it is the extension phone companies that have done the public a disservice. The Commission should review, for example, the extension phone contract obtained from one such service in Fort Worth, Texas.[7] The indemnity clause provides in part:

> . . . . I hereby authorize and empower Second Cellular as my agent to perform the emulation as required on my behalf. I further certify that all equipment connected to this line will be used in a legal manner and <u>hereby agree to indemnify Ellis Communication Corporation, d.b.a. Second Cellular of all liabilities and responsibilities, cost, and expenses which may be incurred by the use of [sic] non-use of this line, phone, equipment, emulation, and enhancements without reservation and I further waive any rights I may have to pursue an action, claim, or suit against Second Cellular and Ellis Communication Corporation due to any act or omission.</u>

Similar indemnity requirements can be found in other such contracts. For example, an almost identical indemnity clause appears in Houston's Cell Time Cellular ("CTC")

---

[7] *See Metroplex Telephone Co. v. Ellis*, No. 3:96-CV-0449-D (N.D. Tex., Feb. 15, 1996). Exhibit A hereto is a copy of the contract.

contract.[8] CTC, of course, admitted fully during court proceedings that it was the exclusive agent of C2+ in the Houston area.[9]

The plain intent of these indemnity provisions is to attempt to shield the C2+ extension phone companies from liability once the consumer learns that use of a cloned extension phone violates both the law and the subscriber contract. No doubt, such drag-net indemnity provisions likely are void as against public policy, but the consumer knows no better until it is too late and any hope of recourse against the extension phone company is gone.

The record also discloses that the extension phone companies have no interest in ensuring the integrity of the operating network. The extension phone cloner in Houston, for example, claimed "there was no limit to the number of extension phones that could be on the same number."[10] He urged the carrier's undercover investigator to get "an additional cellular phone emulated for [his] mother or any other loved one." When told that the investigator's mother lived in Florida, the cloner said "that the emulated phone would still work in Florida in a 'roving-roaming' capacity."[11]

Most of these extension phone companies advise their customers to avoid using their phones at the same time. Of course, the reason to so inform subscribers is to

---

[8] *See* Exhibit B hereto.

[9] *See Houston Cellular Telephone Co. v Nelson*, No, 95-617 (S.D. Tex., Mar. 15, 1995), Stipulation of Facts at 2-3, which states:

> From December 15, 1994 to present Action Cellular Extensions, Inc., was acting, by assignment, as the exclusive distributor in the Houston-Galveston Metropolitan area, of the C2+ Technology, Inc., technology for the emulation and reassignment of the Electronic Serial Numbers in Cellular Telephones, and a provider of the service made possible by that technology. In the regular course of business, a portion of the revenues received as distributor and service provider were remitted to C2+ Technology, Inc.

[10] *See Houston Cellular Telephone Co. v Nelson*, No, 95-617 (S.D. Tex., Mar. 15, 1995), Affidavit of Robert Edwards at 2.

[11] *Id.*

assist them in avoiding detection by the carrier's fraud prevention system, not to preserve the integrity of the operating system. The New York extension phone cloner provided its customers with this special notice:

> It is important to note that ONLY ONE PHONE BE ON AT A TIME. Should more than one phone be on at the same time, you may be in violation of your Carrier's tariffs and in some instances, service may be terminated. DO NOT TAKE BOTH PHONES ON ROAM! FRAUDWATCH Programs WILL DEACTIVATE YOUR NUMBER!!![12]

These cases highlight what C2+ has attempted to obfiscate in all of its submissions: there are fundamental cellular phone service problems inherent in the use of C2+ technology. Again, to use the words of the New York cloner giving advise to its customers: "[i]f two people share one cellular phone number, situations could arise in which the incoming calls could reach the wrong party or be possibly unanswerable, or outgoing calls may not be completed."[13]

The New York cloner company provided specific examples that underscore the fact that the extension phone companies all understand and believe that the extension phones inevitably will be utilized by the subscriber at the same time:

> A. To receive incoming calls it is important that only one designated phone be powered on at any given time. If both phones are on, incoming calls may be unanswerable.
>
> B. If two outgoing calls are being attempted at the same time, it may be that neither call will go through.
>
> C. If a call is in progress on one phone (IN USE) and an outgoing call is attempted on the other phone, the outgoing call

---

[12] *Nynex Mobile Communications Co. v. Cellular Emulation Services*, No. 95 Civ. 4335 (S.D. N.Y. 1995) (attached as Exhibit C hereto).

[13] *Nynex Mobile Communications Co. v. Cellular Emulation Services*, No. 95 Civ. 4335 (S.D. N.Y. 1995) (attached hereto as Exhibit D).

> may not be completed. End call attempt, then try again later. There will be no effect on the call that was originally in progress.
>
> D. If phones will be used by more than one party, it is suggested that a system be devised for their use.[14]

The record reveals that there is no effective way to ensure that a subscriber would not power simultaneously the unlimited number of phones provided by extension phone companies, whether such phones were lawful or not. Not only do such circumstances create inconveniences for cellular customers, they impose tremendous costs on the carrier who undoubtedly will be flooded with complaints about the operating environment and reliability of cellular communications. None of these customer care issues is, or can be, resolved by the C2+ proposals.

In sum, the Commission should view the conduct of C2+ and its franchise companies while the Petition for Reconsideration has been pending as illustrative of the very problems carriers could expect if the Petition was granted even in part. That is, carriers can expect extension phone franchises to mislead subscribers and subscribers to misuse extension phones -- at tremendous cost to the carrier and to the sole profit of C2+ and its licensees.

B. THE TECHNOLOGICAL COST TO SYSTEM INTEGRITY FROM C2+ TECHNOLOGY IS HIGH AND FRAUD WILL FLOURISH

In its ex parte letter of August 11, 1995, C2+ incorrectly asserted that all parties present at the July 1995 meeting "agreed that there is no technical basis for the commission [sic] not permitting an ESN change in the field if a customer requests an extension phone or a [sic] needs a loaner phone."[15] Apparently, C2+ did not hear clearly the position of AWS at the meeting. There is a significant technological and

---

[14] *Id.* (emphasis added).

[15] Independent Cellular Services Association letter to Regina M. Keeney dated August 11, 1995 at 2.

economic cost to both the carrier and the integrity of the operating system directly related to C2+ technology emulation.

The fact that C2+ technology imposes such costs on carriers and damages the network is, in fact, the central point of the Report of Dr. Richard Levine, submitted by C2+ in support of its Petition for Reconsideration. He says that "multiple emulated extension mobile stations are indistinguishable from a single mobile station, as already effectively stipulated by everyone who has commented on this topic, and apparently accepted by the Commission as well."[16] There are at least four major consequences that flow from this striking C2+ admission:

First, as set out in Section A above, that neither C2+ nor the Commission can control subscriber behavior to prevent simultaneous multiple phone usage.[17] Thus, there will always be at least one free cloner call available on the network because carriers will never have the capability of determining whether the second call is a clone or an "extension," absent extraordinarily costly procedures to verify the usage with the customer -- costs apparently to be borne solely by the carrier under the C2+ proposal.

Second, advanced fraud-fighting techniques such as RF "fingerprinting," which creates a distinct RF profile to validate calls for each phone, will not work with extension phones without significant alterations in the current cellular system -- changes again apparently C2+ would have the carrier bear. Otherwise, an emulated phone would lack the RF "fingerprint" associated with the unique ESN/MIN combination of the original unit and would therefore fail the "fingerprint" test and be terminated by the carrier as a cloned phone.

Third, industry standard authentication technology -- the strongest anti-fraud weapon --being deployed by AWS in all of its markets basically renders extension

---

[16] *See* R.C. Levine, "Report on ESN Emulation and Cellular Phone Extension Service" ("Levine Report") submitted by C2+ on July 7, 1995 at 19.

[17] The contrary fiction -- that subscribers will always use but one phone at a time, not that multiple phone registrations is not harmful to the network -- is the house of cards C2+ has built to advance its petition. The extension phone house falls apart immediately and completely once the magnitude of Dr. Levine's and C2+'s admission is understood.

phones unusable in the home area. To accommodate C2+ *and* provide authentication to reduce fraud, carriers once again would either have to re-engineer the authentication industry standard or perform services for C2+ customers to ensure that their "cloned" authenticated phones work on the network. Once again, C2+'s proposal is all risk and liability for the carrier and all reward for itself.

Fourth, introduction of multiple cloned extension phones into the market would violate the Communications Assistance to Law Enforcement Act of 1994 because carriers would be unable to expeditiously isolate calls as required by that Act.[18]

1. The "One Free Clone Phone Call" Rule Resulting from C2+ Technology

The Levine Report is premised mainly on the unsupported proposition that putative subscribers will never use their phones simultaneously.[19] As noted above and demonstrated by the record in the emulation lawsuits, no one can guarantee such consumer behavior and the C2+ companies actually plan for the opposite to occur notwithstanding their public position to the contrary.

The question then becomes what steps will a carrier undertake in the face of wide-spread extension phone deployment. As the Commission knows, carrier anti-fraud measures are designed specifically to detect multiple registration of the same ESN/MIN combination in different parts of the cellular network and to terminate services to those phones. As of February 1995, there were 25 million cellular subscribers and each day 28,000 new customers sign up for services.[20] Even if only a small percentage of that customer base acquired an extension phone through C2+ technology, the current fraud management systems employed by carriers would be challenged beyond capacity to weed out unauthorized calls.

---

[18] Public Law 103-414, 47 U.S.C. §§ 1001-1010.

[19] Levine Report at 1-4.

[20] Cellular Telecommunications Industry Association Wireless Factbook at 6-7 (Spring 1995).

Bluntly put, carriers likely would not challenge simultaneous calls because the cost of doing so would be enormous.[21] This is the "one free clone phone call" rule and it will cost carriers and customers millions of dollars.[22] More to the point, though, the costs associated with this cellular fraud would be borne not by C2+--who would generate the corresponding fraud risk--but by the carriers and their customers.[23]

The problem is magnified by the number of extension phones in service. Nothing in the C2+ submission suggests that there would be only one additional phone per customer available. To the contrary, the rule change proposed by C2+ would permit unlimited extension phones, which would pose unlimited risk to the carrier.[24]

---

[21] This fact is recognized in the Levine Report where he admits that the only solution to the multiple registration problem is for the carrier to "ignore" the simultaneous registrations. Levine Report at 40. This solution, he admits, results in the "customer abandoning a certain very slightly higher level of fraud protection." *Id.* Of course, it is the carrier that bears the risk, not the customer, and the cost to fraud prevention distributed across the network and subscriber base is not slight, but enormous.

[22] The fraudulent use of cellular telephones now costs the industry more than $1 million every day. The cellular telecommunications industry's fraud losses have grown from a $100 million problem in 1991 to more than $365 million in 1994. Although these fraud losses are not charged directly to the cellular subscriber whose phone was cloned, the cost of fraud is passed on indirectly through increased airtime rates Aside from the costs incurred by cellular telephone subscribers, the general public is also at risk from garden-variety criminal activity associated with cloning fraud, including drug trafficking.

[23] Cellular carriers have opposed deployment of the C2+ technology because of its serious compromising of the cellular network and the resulting adverse consequences. Cellular carriers have instead sought to deploy a comparable service that does not undermine cellular system integrity. This has required the development of appropriate software, which must be made consistent with the specific capabilities and technical specifications of the cellular switch in each market where a carrier includes a "cellular extension phone" offering. Thus, the service will be deployed over time where market demands warrant and cellular systems are capable of absorbing the additional services.

[24] "A cellular carrier may not deny service to a cellular subscriber based on the subscriber's use of one or more Secondary Cellular Mobile Stations...." C2+ Proposed Rule Section 22.919(f).

Thus, carriers could be faced with multiple simultaneous registrations of a single ESN/MIN combination. Even if the carrier knew which customers had extensions phone and how many -- a data base solution the building and maintenance cost of which C2+ again would place squarely on the carrier -- there would be no way to determine whether the simultaneous call was a clone or extension phone registration. The most valuable tool in the carrier's fraud fighting arsenal would be lost or the cost of it would soon outweigh its value.

This undeniable impact on the fraud management capability of carriers renders superfluous C2+'s claims that its technology is only utilized by legitimate cellular customers.[25] Obviously carriers have no way of knowing whether multiple registration of ESN/MIN pairs is the result of C2+ emulation, or cloning fraud. Although C2+ finds significant the absence of carrier complaints about C2+ customers engaging in fraud, C2+ itself recognizes that a cellular carrier has no concrete way of identifying the C2+ customer.[26] In fact, cellular carriers routinely terminate service to cellular numbers when the same ESN/MIN combination registers on the system in more than one location. Notwithstanding C2+'s speculation to the contrary, some percentage of these fraud alerts certainly are due to the activities of C2+ customers. The point, however, is that in the future, such fraud alerts would be the norm under the C2+ proposal.

2. RF Fingerprinting Incompatibility

RF "fingerprinting" is an advanced fraud-fighting technique that creates a distinct RF profile to validate calls for each ESN/MIN. Carriers have spent significant funds in the research and development of this tool and it will be deployed around the country shortly.

Unfortunately, RF fingerprinting will not work with extension phones absent a significant investment by carriers in the network to somehow accommodate multiple registrations. Not only will such changes render existing data storage and methodology obsolete, but new systems would have to be developed to accommodate

---

[25] C2+ Petition for Reconsideration at 5.

[26] *See* C2+ Petition for Reconsideration at 9, 12.

extension phone fingerprints. Cross-reference of multiple extension phones in a data base would be required. Maintenance of such a system for current subscription would be necessary. Enrollment by the carrier of each fingerprint into the system would be necessary.

C2+ does not address the cost of these major modifications nor does it propose to pay for the changes. The cost would fall on carriers and customers while C2+ and its cloning companies reaped the pure profit.

3. Authentication Products Render Extension Phone Products Unusable

Authentication is the process whereby the cellular network verifies the claimed identity of the subscriber to protect the network against unauthorized use and theft of services. While it is analogous to a password associated with user ID on a computer, in the cellular environment, the password is "dynamic," changing on every access attempt.

While there are a variety of authentication methods available, authenticating industry standards were developed in 1993 and it has taken industry 4 years to build this complex technology into the cellular phone and network. AWS is in the process of deploying authentication in all of its markets today. The industry standard integrates the ESN as part of the algorithm and it is not transferable between mobile units. Transferring an ESN between two authentication-capable phones will render the "extension" clone inoperable on AWS's network.

Remarkably, C2+'s argument is not that authentication could put them and all other cloners out of business; rather they argue that the Commission should reject the current industry authentication standard because it does not allow for ESN transfers. As Dr. Levine's Report and the C2+ proposed rule demonstrate,[27] C2+ would have the Commission impose a standard that requires transferable authentication modules, much like the European SIM card.

---

[27] *See* Levine Report at 6-8.

Essentially, C2+ asks the Commission to penalize carriers that already have adopted the industry authentication standard and who have incurred significant research, development and deployment costs in an authentication product different than that proposed by C2+ Moreover, C2+ asks for a C2+-only standard so that they can remain in their cloning business. In sum, C2+ asks for nothing less than a complete re-engineering of the authentication standard, the cellular phone product and the network itself for their benefit and at the exclusive cost of carriers.

4. C2+ Will Undermine The Ability Of Carriers To Meet Surveillance Requirements Under CALEA

The Communications Assistance to Law Enforcement Act ("CALEA") was signed into law on October 25, 1994. That law sets forth law enforcement's requirements for the surveillance of wire or electronic communications. Extension phone services as proposed by C2+ will make compliance with CALEA virtually impossible for carriers and will substantially interfere with legitimate law enforcement activities.

Congress enacted CALEA to address the recent and continuing advances in telecommunications technology that have impaired and, in some instances precluded, law enforcement agencies from fully conducting various types of court-authorized electronic surveillance. The primary purpose of CALEA was to clarify a telecommunications carrier's duty to assist law enforcement agencies with the lawful interception of communications and the acquisition of call-identifying information.

To ensure that law enforcement agencies can conduct authorized surveillance of wire or electronic communications, CALEA requires that telecommunications carriers meet the assistance capability requirements.[28] Under Section 103 of CALEA, a telecommunications carrier must ensure that its equipment, facilities, or services are capable of "expeditiously isolating and enabling law enforcement, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission."

---

[28] *See* Section 103 of CALEA (attached hereto as Exhibit E).

A telecommunications carrier must, likewise, ensure that its equipment, facilities, or services are capable of "expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information" before, during, or immediately after the transmission of the wire or electronic communication and "in a manner that allows it to be associated with the communication to which it pertains."

If C2+ were allowed to alter or otherwise manipulate an ESN so that two mobile stations transmitted the same ESN/MIN pair, it would interfere with law enforcement's ability "to intercept, to the exclusion of any other communications," the electronic communications of a subscriber. Carriers would not be able to expeditiously isolate the targeted communication. Even if the extension phone subscriber used only one phone at one time, the result would be the same. There would be multiple phones with the same ESN/MIN and no way to know which phone was in use by whom.

AWS believes that the Commission should solicit the views of the Federal Bureau of Investigation and law enforcement in general on the impact of C2+ technology on electronic surveillance before taking any action on, other than to deny, the Petition for Reconsideration.

C. THE ECONOMIC COST OF EXTENSION PHONE CLONING FALLS SQUARELY ON CARRIERS AND THEIR CUSTOMERS

It should be clear from the above that C2+ is naive at best when they state that C2+ extension phone cloning creates no cost to carriers and only provides benefits to consumers. In essence, what they propose is to profit from the sale of phones that would require a wholesale revamping of the cellular industry while paying none of the costs and assuming none of the risks associated with the changes.

If the C2+ Petition and proposed rule were translated into carrier requirements, AWS would have at least the following obligations:

(1) revamp its fraud management system to ignore multiple registrations from extension phone customers or hire new staff to investigate each simultaneous registration; in any event, increase staff and dedicate more resources to fraud;

(2) retool its RF fingerprinting research and development to accommodate multiple mobile stations, including but not limited to acquiring new software to facilitate cross-referencing, adding data storage capability, provide enrollment access to extension phone companies or add new staff to accommodate enrollment through authorized dealers, add new staff to maintain the extension phone RF data base and to deal with proposed manipulations of ESNs in the field for repairs;

(3) abandon industry standard authentication technology;

(4) increase customer care representatives to deal with customer complaints associated with dropped calls or service denial when two or more extension phones are used at the same time, and to deal with the dissatisfied customers who do not own emulated phones but experience service degradation anyway;

(5) related to (3), determine the manner in which to deliver calls to the subscriber in the event two or more phones are powered on and deal with the customer complaints;

(6) determine what procedures, staff and resources would be required to respond to C2+ extension phone service requests as proposed by C2+, which expects "immediate" response from a carrier if it disagrees with the subscriber status;

(7) determine the changes in equipment and network capacity necessary to meet the assistance to law enforcement requirements of CALEA;

(8) study demands on the system due to emulation and expend resources to adjust capacity to accommodate emulated phones; and

(9) modify subscriber contracts to permit extension phone services.

This simple iteration of obligations imposed on carriers discloses the complexity of C2+ proposal and the fallacy that there are no costs associated with their proposal. In effect, subscribers will pay for extension phone services -- first in the enormous price paid to the extension companies for the virtually costless cloning service and then in the increased price carriers will need to charge for general service to offset the liability and risk incurred as a consequence of the C2+ cloning operations.

D. DEFECTS IN C2+'S PROPOSED RULE UNDERSCORE THE POTENTIAL FOR INCREASED FRAUD AND THE IMPACT ON CARRIERS

AWS does not support any change in Section 22.919. The changes proposed by C2+ would have far-reaching and deleterious effects on carriers and must be rejected.

First, under the C2+ proposed rule, ANY person can clone a phone lawfully. Emulators would not be limited to authorized dealers.[29] The prospect of unlimited, unlicensed cloners lawfully possessing cloning equipment for the putative purpose of creating extension phones serves no valid public policy interest. AWS submits that a much more lucrative market will exist for these "enterprises" if the Commission finds that possession of such cloning equipment no longer carries the inference of fraudulent use for purposes of 18 U.S.C. § 1029.

Second, there would be no monetary or legal relationship between the emulator and the carrier, yet the carrier would be obligated to provide the service and respond to any complaints. What remedies, recourse or protection does C2+ provide for carriers in its rule when extension phone service providers fail to properly instruct subscribers on the use of the extension phone or authorize service improperly? How will the carrier be protected in such a relationship?

Third, C2+ proposed that the carrier bear the immediate risk of subscription fraud. The extension phone company, under the proposed rule, need only call or fax a notice to the carrier of the proposed emulation.[30] There is no requirement to obtain authorization from the carrier; rather, there is a default rule that the emulation can proceed unless the carrier "immediately" objects on one of three limited grounds.[31] Obviously, this procedure is a license for subscription fraud or a mandate for

---

[29] C2+ Proposed Rule Section 22.919(d).

[30] C2+ Proposed Rule Section 22.919(d)(1).

[31] C2+ Proposed Rule Section 22.919(d)(3).

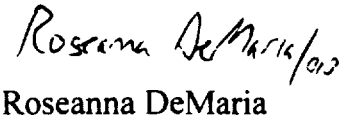
increased staffing and resource requirements within the carrier organization to service the C2+ business without compensation.

Fourth, C2+ places the entire burden on the carrier to police the system for simultaneous registrations and then authorizes the carrier in the proposed rule to terminate service for such usage.[32] Yet C2+ has taken great pains to convince the Commission that such multiple registrations will not occur. This proposed rule language speaks volumes about the likely misuse of the network by subscribers using C2+ technology. The proposed rule also places the full burden on carriers to develop procedures and rules of suspension and termination for the inevitable misuse of the system. Once again, C2+ would profit while the carrier and customer would pay.

E. CONCLUSION

For all of the reasons set forth in this letter, the Commission should act now to reaffirm its commitment to ensuring that carriers possess the tools to fight cellular fraud. Further, the Commission should reject the profiteering proposal of C2+ and protect carriers and customers alike from widespread cloning operations that would undermine the integrity and foundations of the entire industry. AWS remains available to answer any questions concerning this submission and to provide any further information as needed.

Very truly yours,



Roseanna DeMaria
Vice President, Business Security

Enclosures

---

[32] C2+ Proposed Rule Section 22.919(e).