

EX PARTE OR LATE FILED

WILEY, REIN & FIELDING

1776 K STREET, N. W.
WASHINGTON, D. C. 20006
(202) 429-7000

FILED 0
OCT 27 1
FBI

JEFFREY S. LINDER
(202) 429-7384

FACSIMILE
(202) 429-7049
TELEX 248349 WYRN UR

October 25, 1994

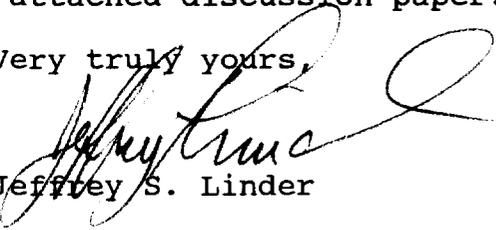
William F. Caton
Acting Secretary
Federal Communications Commission
1919 M Street, N.W.
Washington, D.C. 20554

Re: Ex Parte Contact in Docket No. 93-292

Dear Mr. Caton:

This is to inform you that Scoop Sairanen, Vice President-Regulatory of TCA, and I met with Linda Dubroof and other members of the Enforcement Division staff to discuss toll fraud. We handed out the attached discussion paper.

Very truly yours,



Jeffrey S. Linder

JSL:rw

cc: Linda Dubroof

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

0

FCC POLICIES CAN REDUCE TOLL FRAUD

RECEIVED

OCT 2 1994

Fundamental Realities

- Toll fraud is roughly a \$5 billion dollar annual problem -- and is continuing to increase
- Users are poorly situated to identify and control fraud on a network-wide basis -- but are held solely responsible for fraudulent charges
- The marketplace is not working to minimize fraud -- users do what they can, but carriers have little incentive to help
- Insurance is not the answer -- policies have high deductibles and huge coverage gaps

Breaking the "Fraud Chain"

- *LECs* should be required to provide international call blocking to all business customers; federally tariff Originating Line Screening and Billed Number Screening; and preserve the use of "1" as a toll indicator
- *IXCs* should be required to make real-time monitoring universally available as an inherent part of fraud-susceptible services and to provide explicit warnings of the fraud risks associated with particular services
- *Manufacturers* should be required to provide warnings and to advise customers what features may be utilized to minimize fraud, and should be given incentives to incorporate deterrents to fraud and to increase the security of the remote access maintenance port.

- *Customers* should be insulated from liability if they take appropriate steps to limit exposure to fraud, including maintaining accurate lists of all employees and addresses getting remote maintenance and DISA authority; controlling the transfer of codes; providing timely notification to the carrier to disable a code when the customer believes it is compromised; following the carrier's and manufacturer's recommendations regarding code length, frequency of changing codes, and use of silent prompts; including these obligations in any PBX maintenance contract; and cooperating with the carrier to investigate and prosecute instances of unauthorized usage.

Rationalizing Liability

- Customers should not be held liable for unauthorized usage charges where they have discharged the above obligations and the fraud was not perpetrated or assisted by an employee
- Where fraud is assisted by an employee, the user's liability should cease fifteen minutes after it notifies the carrier to disable the code.
- Where a customer may legitimately be held liable for unauthorized usage, it should pay only the carrier's out-of-pocket costs -- not profits.
- Manufacturers should be held liable for fraud perpetrated through the remote access maintenance port of a PBX