NATIONAL DEFINITY® Users Group

National DEFINITY® Users Group, Inc. P.O. Box 2167 • Indianapolis, Indiana 46206-2167

Past-President
Sally York

U.S. Leasing International
733 Front Street MS10
San Francisco CA 94111
415-627-9084

EX PARTE OR LATE FILED

DOCKET FILE COPY ORIGINAL

February 23, 1994

RECEIVED BY
FEB 24 1994
FCC - MAIL ROOM

Mr. William Caton
Acting Secretary
Federal Communications Commission
Washington, D.C. 20554

RE: Reply Comments on Docket No. 93-292

Dear Mr. Caton:

I am writing on behalf of the 2,200 members of the National DEFINITY® and Global DEFINITY® Users Groups. Seventy-five percent of the comments received on Docket No. 93-292 were from members of the National DEFINITY® and Global DEFINITY® Users Group. As we stated in our letters, we believe the FCC was on the mark in proposing shared liability for toll fraud losses. Based on the sheer volume of letters sent from our groups, it proves this is an issue that is of extreme importance to us. We have not employed expensive lawyers to represent our position. We speak from the trenches, so to speak, of the growing problem of toll fraud.

We were not surprised to read that MCI, AT&T, Sprint, WilTel, BellSouth, South Western Bell, Pacific Bell, U.S. West; et al, were opposed to shared liability. They state that "the customer is in the best position to detect and prevent fraud and should be given the financial incentive to do so." Doesn't the customer already have the incentive? And because of this, has toll fraud ceased to be a problem? No, because the customer cannot stop fraud completely without the help of the IXCs, LECs and CPE vendors. Shared liability would encourage all parties (customers, IXCs, LECs and CPE vendors) to do all they can to prevent fraud so that they will not have to pay for it. The more parties in prevention, the stronger the lines of defense.

We agree with NATA who states, "Those who commit toll fraud look for the weak points that allow access. When one potential access point is "plugged" by installing improved CPE, toll fraud criminals move on to the next. It is unrealistic to expect that every potential access point, i.e. every business telecommunications system - or even a majority of them could be effectively shut off from fraud in the foreseeable future. Therefore, while an important contribution to preventing toll fraud can be and is being made by CPE safeguards, such safeguards can never have the same 'bang for the buck' as improved safeguards in the network."

No. of Copies rec'd 0+2
List ABCDE

NATA also states, "The current 'system' for assigning liability for toll fraud puts all the onus on 'customers,' who cannot reasonably be expected to take the lead in preventing fraud. It is unrealistic to expect each of hundreds of thousands of business users, who generally have no particular telecommunications expertise, to take the time to educate themselves about fraud, to try to figure out what they need to add to their CPE or network services in order to prevent as much fraud as possible, and to spend the money to bring each of their individual locations up to state-of-the-art fraud protection. The current system relies on litigation to bring customers into line, and it has imposed excessive costs on them, as well as generating a lot of unnecessary stress, ill will, and confusion throughout the community of business end users."

The assumption that only users can be fully responsible for their PBX systems is absurd. In the first place, fully half of the members of the National DEFINITY® Users Group have only part-time telecommunications responsibilities. Many are not telecommunications professionals. Equipment manufacturers such as AT&T are now marketing PBXs with line size capacities under 50 that are aimed at small companies that may have no telecommunications staff whatsoever. Equipment manufacturers must be responsible for training and informing all users about the dangers of toll fraud. Telecommunications systems must also be installed and implemented in the most secure fashion possible. Financial risk will encourage them to do so. It is ridiculous to put the burden of reviewing real-time calling statistics and patterns on the backs of the users. They do not have the systems, personnel or expertise to accomplish this task. The LECs and IXCs have it within their means to provide this service for all customers.

To further illustrate the point that users do not have complete control over their equipment here are some examples:

> **Scenario 1:** A CPE owner has the Remote Access feature "turned off" and takes steps to monitor traffic on a daily basis to look for fraud patterns. A hacker gains access to the maintenance port of the CPE owner's PBX utilizing the PBX vendor's high level maintenance password. The hacker then turns on Remote Access and on a Friday night turns off the call monitoring capability. The PBX is hacked all weekend until early Monday morning when the call monitoring capability is turned back on. The unsuspecting CPE owner runs toll fraud reports for the weekend and shows no activity. This fraudulent activity goes on full force until the CPE owner gets the bill via a UPS truck.

The IXCs and/or LECs will see these fraudulent calls long before the customer, despite their claim that they are not familiar with a particular customer's calling patterns. Fraudulent calls vary little in their patterns. The CPE manufacturer is the responsible party for controlling access to their maintenance password. Yet, according to current law it is the PBX owner who will carry the full burden of the fraud that occurs.

> **Scenario 2:** PBX owners only have limited call monitoring capability. Hackers are clever and are always devising new methods of breaking in. Many PBX owners are

monitoring calls to known toll fraud regions such as the Dominican Republic or South America. Hackers are aware of this so now when they break in to a PBX they call the U.K. or Australia, break in to a system there and then call the Dominican Republic or South America. Many companies in the U.S. conduct business with the U.K. and Australia, which makes these types of calls harder to detect as fraudulent calls.

Scenario 3: LECs continuously assign new prefixes like the 976 pay per call prefix. There are no updates to customers warning of these prefixes so they can be blocked in the PBX. These 976 look-alike numbers are a important factor in "pay call" scams. Persons imitating couriers enter offices announcing they are there to pick up or deliver a package for an individual. After being advised no such person worked at the location, the "courier" will feign surprise and ask to make a local call to their office. The "local call" is to a "pay call" service which can charge $75 to $250 per minute. The "courier" will stay on the phone a couple of minutes and then leave. The LECs do very little to stop this type of fraud because they profit these calls.

Scenario 4: It is assumed that the customer is the only one with authorized administrative access to a PBX. Yet, many customers have service contracts. These service providers often times leave the system vulnerable because they are service oriented, not security oriented. Hackers are very bright, intelligent and creative individuals. When they can, they will mask how they penetrate the system through the customer permission levels.

Sound far fetched? Not at all. These examples are not uncommon and are just a few to point out that the customer cannot completely control their environment as it relates to the protection of fraud. Many of these scenarios may look at first glance as customer negligence, but deeper investigation would prove otherwise.

AT&T testified at the Congressional Oversight Hearing on Toll Fraud in June of 1992 that the first documented case of PBX fraud was in 1979, and yet it wasn't until 1992 that the carriers responding from pressure from Congress and the FCC developed their monitoring and insurance programs. They were forced to improve security measures.

In fact, it wasn't until the carriers were losing money on calling card fraud that they increased fraud measures and monitoring capabilities to spot fraud attempts. When these changes occurred, it shifted the fraud occurrences on to the premise equipment. With this shift, customers as well as CPE vendors were totally unprepared for this. As recently as 1993, there was no mention of the risks from toll fraud in any PBX documentation nor was it discussed in the training provided by CPE vendors. And yet all these respondents believe customers must have some sort of intuitive sense about fraud and how to prevent it. Countless PBX systems are installed by the CPE vendors with default passwords, risk prone features activated by the vendor and nothing is said to the customer about these risks.

Even when we exercise due diligence in closing down the PBX, hackers continue to migrate with new technologies. When this happens, we can't be held accountable. The IXCs, LECs and CPE vendors are in the best position to track the new hacker methods. The customer is always the last to know.

Customers bear 100% of the liability today, regardless of who has responsibility. Full liability on their part has not eliminated fraud. Customers cannot be fully liable for the intimate workings of PBX technology and the network services it is attached to. The manufacturers must have a responsibility to inform users of potential threats and the means to combat them. This must apply to the full installed base, not just to new products and services. The IXCs can easily develop systems to identify fraud more quickly and more accurately to reduce losses. The LECs need to start screening their customers better to identify 976, 800 call scams, and call-sell operations.

Customers who have purchased a new PBX within the last year can well see the security enhancements made by the CPE vendors. But what about those customers with older equipment. Who is telling them about fraud? NATA and Northern Telecom stated it would be "too burdensome" to have to warn their embedded base. If they don't, then who will?

As PBX owners, we are willing to step up to our responsibilities but we cannot win the war on toll fraud alone. We must have the cooperation and support of the IXCs, LECs and CPE providers. We cannot stop fraud by ourselves. We are asking for a FAIR and EQUITABLE ruling by the FCC which will help us in the defense of fraud and not an arbitrary ruling that makes the customer 100% liable for the cost of fraud.

Sincerely,

Sally York
Past President & Security Committee Member
National DEFINITY® Users Group

cc: U.S. Representative Edward J. Markey

Member Companies Responding to Docket 93-292

University of Oklahoma
Mercy Healthcare, Inc.
El Paso Water Utilities
Connie North
AmSouth
Bessemer & Lake Erie Railroad Company
Central Products Company
H.B. Zachry
Ernst & Young
Greeley Medical Clinic
Brunschwig & File
West Georgia Medical Center
Himont
FOG
Westvaco
Global DEFINITY
Joan McCarthy
Liberty Diversified Industries
UMI
Green Point Saving Bank
Specialized Bicycle Components
C.R. Bard, Inc.
Kim Norby
LTV Steel Company
United Fire & Casualty Company
OBICI
Milbank, et al
Pace Foods, Inc.
Wm. C. Brown Communications, Inc.
BHK&R, Inc.
Keystone
Mid-America Group
Thomas Hospital
South Seas Resorts Company
Pennock
Agribank
Wilkerson Group, Inc.
Legent Corp.
Crawford & Company
Delaware Valley Medical Center
M.D. Health Plan
UTC
Northrup King Company

National DEFINITY Users Group
Halliburton Company
Indiana University
Indiana Medical Referral
USL Capital
Holyoke Mutual Insurance Company
Colgate-Palmolive
Liberty Financial
Doreen M. Nealon
Bechtel
Charles River Laboratories
Albany International
Plumbing Claims Group, Inc.
Washington Education Association
Iowa Farm Bureau Federation
Universal Gym Equipment, Inc.
Prince
The News Journal Company
Pioneer Hi-Bred International, Inc.
South East Alaska Regional Health Corporation
Cameron & Barkley Company
King County Fire Protection District No. 39
Suntrust Service Corporation
Mid-Continent LIfe Insurance Company
O'Sullivan Corporation
Dana Victor Products Division
Advanced Micro Devices
ITT Residential Capital Corporation
East-West Center
Clopay Corporation
Edgewood College
Olin
Cap Gemini America
St. Margaret's Hospital
Watlow Electric Manufacturing Company
Textron Marine Systems
Jos. R. Newberry Jr.
Merck & Company
Andersen Consulting
ITC
Central States Can Company
Robert-Wood-Johnson University Hospital
Madison Area Technical College
Schneider National
Cheif H. Fitchey
Schinder Elevator Corporation

Nila J. P. Didonna
Lyondell Petrochemicals Company
Resolution Trust Corporation
Sea-Ray Boats, Inc.
Arthur Andersen & Company
Virginia Murphy
Raytheon Service Company
Gardner Denver Machinery, Inc.
Dover Elevators
Southeast Missouri State University
Moore Research Center
Mercy Health Center
3M
Debby Earhart
CareerTrack
Barbara Turner
Ohio Historical Society
Northern Trust Bank
HIP of Greater NY
Thomas Cook Travel
Delmar Fair
Betty Warren/Procter & Gamble
Central Steel & Wire Company
City of St. Petersburg
Cape Industries
Ball Corporation
Countymark Cooperative, Inc.
Brenda Williams
Davis County Information Systems
Beechcraft
The ESAB Group
P. McLemore/Solar Turbines, Inc.
Fran Anaya/W.L. Gore & Assoc.
Deborah Winburn
Donald Murphy/Children's Hospital of PGH
BMD
Boise Cascade Corporation
Julie McDrake
Vern Olson/Utah County
Wunderman Cato Johnson
Chiquita Brands International
Barbara Dworak/Dean Witter Discover & Co.
Sentara Health System
Al Lopez/Rose Medical Center
Eastern Idaho Regional Medical Center
Jennifer Olewee

Lab Safety Supply
Rick House
Bechtel/Jane Reber
Group Health Cooperative
Clopay
MHG Memorial Hospital
Allendale Insurance
Borden
Board of Education of the City of New York
Patricia Weyl/W.L. Gore & Assoc.
Beaumont
Dale Mathis
Sandy Cox/Tx Guaranteed Student Loan Corporation
Rowe International, Inc.
Dayton Extruded Plastics
City of Tempe
Grolier Inc.
James River Corporation
Baxter
Kelly Lister/QVCTE
The Prudential
City of Amarillo
Thomas Zona/Charming Shoppes
Ocean Reef Club
Polly Martin/The Boston Company
Carpenter Technology Corporation
John Deer Life Insurance Company
Raymun Strickland/Superior Court of DC
Jane Zaunter/Rudolph Libbe, Inc.
The George Washington University
Dunkin Donuts
Arch Mineral Corporation
Carle Clinic Association
Fisons
Vermont National Bank
Mount Carmel Corporate Services
Diane Peterson
Memorial Medical Center, Inc.
Courtaulds Aerospace
World Financial Network National Bank
Nancy Graven/ARA Services, Inc.
ORIX USA Corporation
Mount Carmel Corporate Services
Crestar Bank
Alan Grady Jones/Texas Commerce Bank
Linda Mazzorella

The Toro Company
Rod McNeill
PriMerit Bank
Frank G. Villarmia, Jr./Amstar Communications
Antioch Publishing Company
Invesco Funds Group
Keni Bailey/Infirmary Health System
SCRA
John Wood/Citibank, SD
Anthony Delfino
CACI
Community Health Plan
America West Arena
University of Pittsburgh
R.D. Marsh
Viewlogic
Tony Barron
The Children's Hospital/Denver, CO
Residential Services Corporation of America
Jeff S. Rupp
The Illinois State Toll Highway Authority
Brenda Farris
Alvin Erd/Warner Lambert
Tetley, Inc.
New Jersey Natural Gas Company
North American Mortgage Company
Stone & Webster Engineering Corporation
A.J. Bond
Nancy G. Kleine/Saint Anthony Med Center
Glenda Galukat
Employers Reinsurance Corporation
Middlesex Mutual Assurance Company
Ingram Book Company
Maritz, Inc.
McDermott, Will & Emery
Atmos Energy Corporation
Lou Gands/GE Aircraft Engines
Brenda Voigtritter/SAIC
Farmland Industries, Inc.
Belz Enterprises
Edie Kassabean/CHCC
Great West Life & Annuity
Pitney Bowes
Huls America, Inc.
Keith Fitts
Employers Health Insurance

Arrow Uniform Rental, Inc.
Exxon Chemical
American Mutual Life Insurance Company
Leonard Cedo, Jr./Brooklyn Union Gas Co.
Boeing Employees Credit Union
Blue Cross/Blue Shield of Texas
Vincent Dibble/Musc
General Mills, Inc.
North Pacific Insurance Company
California State University
Valley International Airport
Martin Memorial Health Systems, Inc.
O.F. Mossberg and Sons, Inc.
Dun & Bradstreet Ltd.
Sacred Heart Medical Center
Sandy Patrick/Intel
Pat Beadle
Behlen MFG Co.
First Data Corp.
Laramie County Government
Allegheny Intermediate Unit
Laurie Steenhoon
National Jewish Hospital
Blessing Hospital
Eaton Corporation
Monarch Marking Systems, Inc.
University of Connecticut
Century Companies
United Missouri Bank
Minnesota Mutual
Praxair
Elizabeth Duncan
County of El Dorado
Woman's Hospital