



# QUEEN OF THE HACKERS

## COMMENT

### Cut and paste

The new National Curriculum requires schoolchildren to be familiar with computers: word processing, database and spreadsheet management and so on.

Now the Government cuts spending on information technology education by £5 million - by nearly a half.

This will reduce the number of advisory IT teachers by a similar margin, thus putting more pressure on already overworked teachers who will presumably be expected to take more of the computer teaching responsibility themselves.

Learning to use a computer is far more complicated than learning to drive. Few people would want their children to be taught to drive by someone just learning to drive themselves, yet it seems that computing is to be taught by people who are just picking up the subject on their own (probably in their own time too).

Computers can be an invaluable time and tedium-saving tool - any micro owner can tell you that. They can be a legitimate leisure tool. But they can also degenerate into a glorified toy. If children don't get the right impression first off they will treat computers as a mystical box of tricks that can play nice games which are far more interesting than the patchily taught and boring 'proper' uses being demonstrated in lessons.

Time and again Britain has lost out because of insufficient investment in education and technology. If cuts like this are made at such a grass roots level it is difficult to see how any amount of training investment made later by trade and industry is going to remedy things.

A Chicago based woman faces ten years in jail after allegedly recruiting impressionable youngsters to defraud large companies by computer hacking.

Lynn Doucett has been accused of setting up a network of 60 teenagers throughout the US who were employed to hack into computers and obtain people's credit numbers which they then used to access services. Doucett, 35, then pocketed some \$1.5 million raised by the teenagers, some of whom were as young as 14.

She is currently being detained in Chicago charged with computer fraud - her trial is pencilled in for early August. Some of the young hackers are also being charged although they will not be incarcerated.

Like Charles Dickens' devious Fagin she set about exploiting the dubious talents of youngsters for her own

ends, say US secret service agents. Doucett made contact with the teenagers by logging onto bulletin boards around the country. She then taught them how to hack into computers and told them which networks to break into.

US Secret Service agent James Huse - who helped track Doucett down - told Express: "She was the leader of a national conspiracy which at one time consisted of about 60 young hackers. This is the largest hacking network I've ever come across."

He said: "She got them intrigued by the prospect of gaining access over telephone lines to forbidden places. For them it wasn't defrauding anybody. It was just playing a game."

Secret Service agents (who are responsible for tackling computer crime in the US) were alerted to the operation when various companies found they had been defraud-

ed. They followed Doucett because she is well known as "an old hand at white collar crime". She was previously convicted of computer fraud in Toronto.

"When we began our investigation we assumed that we

would find adults sending out the phoney orders," said Huse. "We were jolted to discover the kids were 14 year-olds. This woman was exploiting their fascination in a new medium. We all hate to see kids getting involved in something like this."

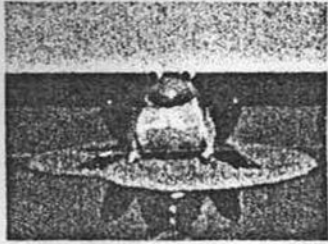
Leading the case was Chicago-based secret agent Mike Cleary. He told Express: "We tracked back some of the hackers after they had penetrated various systems and found her to be at the centre of the operation. We arrested her last April and she's now being detained at the Metropolitan Correction Centre in Chicago.

"We call her the Queen of the Hackers."

## Arting around

Budding Amiga artists now have the chance to show off and win some exciting prizes by entering the Edinburgh International Festival 2nd Computer Animation Competition.

Leading Commodore hardware and software distributor Amiga Centre Scotland is again organising the competition, with the finalists entries due for display at the Computer Animation Exhibition.



Closing date for the entries - which can be on disk or PAL VHS videotape - is 24th August. Further details from Amiga Centre Scotland on 031 5574242.

• Spawning a masterpiece: Can you beat this?

## Amstrad the benevolent

Amstrad's first venture into charity sponsorship has raised a tasty £165,000 for the Muscular Dystrophy Group.

Boss Alan Sugar was in the thick of the Amstrad Pro-Celebrity tennis tournament. Indeed, the tough tycoon managed to win along with Vijay Amritraj stuffing Terry Wogan and John Lloyd in the process.

Other names on hand included Frank Bruno, Jimmy

Tarback, Janet Street-Porter and Nigel Dempster. Sir Richard Attenborough - who is president of the MDG - presented the silverware to the winners.

Although Sugar is said to be extremely generous in private to worthwhile causes this is the first time his usually surly company has openly backed a charity. ■



• Sir Richard, Amritraj, and Sugar - winning for charity

## SNIPPETS ● SNIPPETS ● SNIPPETS

● A new monthly magazine is to be published concentrating on the virus problem. Virus Bulletin will be full of editorial and will include contributions from various experts. More on 0844 290396...

● Tandy tells us that all the unsavoury hacks covering this year's Wimbledon are using its special computer support service. The journoes are basically doing their thing on Tandy portables and then wiring it through to the sports desk.

● Business software firm Lifetree has undergone a simultaneous management buy out in the UK and its US offices...

● Clares has just finished a sequence of animations for HTV Wales put together on the Archimedes. The work was done for a new Welsh language quiz show. It features aeroplanes flying around and scrolling background. Clares was responsible for work on kiddies show Going Live...

## This is the modem world

Portable PC owners can now send and receive data on the move via cellular telephone and the latest cellular modem from Rascal-Vodafa.

Weighing in at 710g (1.5lbs), the £600 modem allows you to communicate with other modem users and access networks like Micronet and Prestel. Even in severe reception conditions, data throughput is claimed to be sharp.

With full autodial/ autoanswer facilities, the modem has a low power consumption, minimising any reduction of "talk-time" on battery-powered Vodafones. According to Rascal-Vodafa, the CDLC modem brings the "portable office" one step closer - the unit is itself certainly small enough to make little difference to anyone already carrying a portable computer and Vodafone.

Versions of the modem compatible with the the NEC 11A and Panasonic C series of cellular telephones are available now, and others for the Autoline and new Talkman ranges from Nokia Mobira and the MCR40 from Philips are on the way. An NEC 9A version is also under development, and the modems will thus cover nearly 40% of the total Vodafone subscriber base.

Nomadic executives can find out more on 0635 33251. ■

- EDITOR Rob Ainsley
- NEWS EDITOR Colin Campbell
- FEATURES EDITOR Andy Storer
- REVIEWS EDITOR Rik Haynes
- TECHNICAL EDITOR Jerry Glenwright
- ART EDITOR Angela Neal
- ART ASSISTANT Harriet Athay
- PRODUCTION EDITOR Rod Lawton
- ADVERTISMENT MANAGER Mark Salmon
- AD EXECUTIVES Sarah King, David Lilley
- AD TYPESETTING Terry Turner
- PUBLISHER Greg Ingham

© Future Publishing Ltd  
4 QUEEN ST, BATH, BA1 1EJ  
TEL: 0225 446034 • FAX: 0225 446019 Printed by Redwood Web Offset, Trowbridge, Wilts Distributed by Comag, West Drayton, Middx

another \$11,500—to say nothing of the cost of registering PC Cyborg Corporation in Panama, or establishing an address in London. To add insult to injury, not one license payment was ever received from anyone, anywhere.

Popp's scheme was not particularly well thought out. The scam depended on recipients of his diskettes mailing checks halfway around the world in the hope of receiving an antidote to the trojan. But, as John Austen said, "Who in their right mind would send money to a post office box number in Panama City for an antidote that might never arrive?" Or that may not be an antidote anyway.

It seems unlikely that anyone will ever again attempt a mass blackmail of this type; it's not the sort of crime that lends itself to a high volume, low cost formula. It's far more likely that specific corporations will be singled out for targeted attacks. Individually, they are far more vulnerable to blackmail, particularly if the plotters are aided by an insider with knowledge of any loopholes. An added advantage for the perpetrators is the likely publicity blackout with which the corporate victim would immediately shroud the affair: every major corporation has its regular quota of threats, mostly empty, and a well-defined response strategy.

But at present, hacking—which gives access to information—has proven to be substantially more lucrative. Present-day hackers traffic in what the authorities call access device codes, the collective name for credit card numbers, telephone authorization codes, and computer passwords. They are defined as any card, code, account number, or "means of account access" that can be used to obtain money, goods, or services. In the United States the codes are traded through a number of telecom devices, principally voice-mail computers; internationally, they are swapped on hacker boards.

The existence of this international traffic has created what one press report referred to colorfully as "offshore data havens"—pirate boards where hackers from different countries convene to

trade Visa numbers for computer passwords, or American Express accounts for telephone codes. The passwords and telephone codes, the common currency of hacking, are traded to enable hackers to maintain their lifeline—the phone—and to break into computers. Credit card numbers are used more conventionally: to fraudulently acquire money, goods, and services.

The acquisition of stolen numbers by hacking into credit agency computers or by means as mundane as dumpster diving (scavenging rubbish in search of the carbons from credit card receipts) differs from ordinary theft. When a person is mugged, for example, he knows his cards have been stolen and cancels them. But if the numbers were acquired without the victim knowing about it, the cards generally remain "live" until the next bill is sent out, which could be a month away.

Live cards—ones that haven't been canceled and that still have some credit on them—are a valuable commodity in the computer underworld. Most obviously, they can be used to buy goods over the phone, with the purchases delivered to a temporary address or an abandoned house to which the hacker has access.

The extent of fraud of this sort is difficult to quantify. In April 1989 *Computerworld* magazine estimated that computer-related crime costs American companies as much as \$555,464,000 each year, not including lost man-hours and computer downtime. The figure is global, in that it takes in everything: fraud, loss of data, theft of software, theft of telephone services, and so on. Though it's difficult to accept the number as anything more than a rough estimate, its apparent precision has given the figure a spurious legitimacy. The same number frequently appears in most surveys of computer crime in the United States and is even in many government documents. The blunt truth is that no one can be certain what computer fraud of any sort really costs. All anyone knows is that it occurs.

Leslie Lynne Doucette has been described as "the female Fagin" of the computer underworld. In her mid-thirties, she was consid-

erably older than the 150 or so adolescent Olivers she gathered into her ring. As a woman, she has the distinction of being one of only two or three female hackers who have ever come to the attention of the authorities.

In 1989 Doucette lived in an apartment on the north side of Chicago in the sort of neighborhood that had seen better days; the block looked substantial, though it was showing the first signs of neglect. Despite having what the police like to term "no visible means of support," Doucette was able to provide for herself and her two children, pay the rent, and keep up with the bills. Her small apartment was filled with electronic gear: personal computer equipment, modems, automatic dialers, and other telecom peripherals.

Doucette was a professional computer criminal. She operated a scheme dealing in stolen access codes: credit cards, telephone cards (from AT&T, MCI, Sprint, and ITT) as well as corporate PBX telephone access codes, computer passwords, and codes for voice-mail (VM) computers. She dealt mostly in MasterCard and Visa numbers, though occasionally in American Express too. Her job was to turn around live numbers as rapidly as possible. Using a network of teenage hackers throughout the country, she would receive credit card numbers taken from a variety of sources. She would then check them, either by hacking into any one of a number of credit card validation computers or, more often, by calling a "chat line" telephone number. If the chat line accepted the card as payment, it was live. She then grouped the cards by type, and called the numbers through to a "code line," a hijacked mailbox on a voice-mail computer.

Because Doucette turned the cards around quickly, checking their validity within hours of receiving their numbers and then, more importantly, getting the good numbers disseminated on a code line within days, they remained live for a longer period. It was a very efficiently run hacker service industry. To supplement her income, she would pass on card numbers to members of her ring in other cities, who would use them to buy Western Union

money orders payable to one of Doucette's aliases. The cards were also used to pay for an unknown number of airline tickets and for hotel accommodation when Doucette or her accomplices were traveling.

The key to Doucette's business was communication—hence the emphasis on PBX and voice-mail computer access codes. The PBXs provided the means for communication; the voice-mail computers the location for code lines.

PBX is a customer-operated, computerized telephone system, providing both internal and external communication. One of its features is the Remote Access Unit (RAU), designed to permit legitimate users to call in from out of the office, often on a 1-800 number, and access a long-distance line after punching in a short code on the telephone keypad. The long-distance calls made in this way are then charged to the customer company. Less legitimate users—hackers, in other words—force access to the RAU by guessing the code. This is usually done by calling the system and trying different sequences of numbers on the keypad until stumbling on a code. The process is time-consuming, but hackers are a patient bunch.

The losses to a company whose PBX is compromised can be staggering. Some hackers are known to run what are known as "call-sell" operations: sidewalk or street-corner enterprises offering passersby cheap long-distance calls (both national and international) on a cellular or pay phone. The calls, of course, are routed through some company's PBX. In a recent case, a "call-sell" operator ran up \$1.4 million in charges against one PBX owner over a four-day holiday period. (The rewards to "call-sell" merchants can be equally enormous: at \$10 a call some operators working whole banks of pay phones are estimated by U.S. law enforcement agencies to have made as much as \$10,000 a day.)

PBXs may have become the blue boxes for a new generation of phreakers, but voice-mail computers have taken over as hacker bulletin boards. The problem with the boards was that they became too well known: most were regularly monitored by law

enforcement agencies. Among other things, the police recorded the numbers of access device codes trafficked on boards, and as the codes are useful only as long as they are live—usually the time between their first fraudulent use and the victim's first bill—the police monitoring served to invalidate them that much faster. Worse, from the point of view of hackers, the police then took steps to catch the individuals who had posted the codes.

The solution was to use voice mail. Voice-mail computers operate like highly sophisticated answering machines and are often attached to a company's toll-free 1-800 number. For users, voice-mail systems are much more flexible than answering machines: they can receive and store messages from callers, or route them from one box to another box on the system, or even send one single message to a preselected number of boxes. The functions are controlled by the appropriate numerical commands on a telephone keypad. Users can access their boxes and pick up their messages while they're away from the office by calling their 1-800 number, punching in the digits for their box, then pressing the keys for their private password. The system is just a simple computer, accessible by telephone and controllable by the phone keys.

But for hackers voice mail is made to order. The 1-800 numbers for voice-mail systems are easy enough to find; the tried-and-true methods of dumpster diving, social engineering, and war-dialing will almost always turn up a few usable targets. War-dialing has been simplified in the last decade with the advent of automatic dialers, programs which churn through hundreds of numbers, recording those that are answered by machines or computers. The process is still inelegant, but it works.

After identifying a suitable 1-800 number, hackers break into the system to take over a box or, better, a series of boxes. Security is often lax on voice-mail computers, with box numbers and passwords ridiculously easy to guess by an experienced hacker. One of the methods has become known as finger hacking: punching away on the telephone keypad trying groups of numbers until a box and the appropriate password are found. Ideally, hackers

look for unused boxes. That way they can assign their own passwords and are less likely to be detected. Failing that, though, they will simply annex an assigned box, changing the password to lock out the real user.

VM boxes are more secure than hacker boards: the police, for a start, can't routinely monitor voice-mail systems as they can boards, while hackers can quickly move to new systems if they suspect the authorities of monitoring one they are using. The messaging technology of voice-mail systems lends itself to passing on lists of codes. The code line is often the greeting message of the hacker-controlled mailbox; in other words, instead of hearing the standard "Hello, Mr. Smith is not in the office. Please leave a message," hackers calling in will hear the current list of stolen code numbers. In this manner, only the hacker leaving the codes need know the box password. The other hackers, those picking up the codes or leaving a message, only need to know the box number.

It was ultimately a voice-mail computer that led the authorities to Doucette. On February 9, 1989, the president of a real estate company in Rolling Meadow, Illinois, contacted the U.S. Secret Service office in Chicago. His voice-mail computer, he complained, had been overrun by hackers.

The harassed real estate man became known as Source 1. On February 15th, two Secret Service agents—William "Fred" Moore and Bill Tebbe—drove from Chicago to the realtor's office to interview him. They found a man beset by unwanted intruders.

The company had installed its voice-mail system in the autumn of 1988. The box numbers and passwords were personally assigned by the company president. While the 1-800 number to access the system was published, he insisted that the passwords were known only to himself and to the individual box users.

In November 1988, during an ordinary review of the traffic on the system, he had been startled to discover a number of unexplained messages. He had no idea what they were about or who they were for; he thought they could have been left in error.

However, the number of "errors" had grown throughout November and December. By January 1989 the "errors" had become so frequent that they overwhelmed the system, taking over almost all of the voice-mail computer's memory and wiping out messages for the company's business.

The Secret Service recorded the messages over a period from late February to March. Listening to the tapes, they realized they were dealing with a code line.

The law on access devices prohibits the unauthorized possession of fifteen or more of such codes, or the swapping or sale of the codes "with an intent to defraud." (Fraud is defined as a \$1,000 loss to the victim or profit to the violator.) On the tapes, the agents could identify 130 devices that were trafficked by the various unknown callers. They also heard the voice of a woman who identified herself alternatively as "Kyrie" or "long-distance information." It seemed as if she was running the code line, so they decided to focus the investigation on her.

In March security officials from MCI, the long-distance telephone company, told the Secret Service that Canadian Bell believed "Kyrie" to be an alias of Leslie Lynne Doucette, a Canadian citizen who had been hacking for six or seven years. In March 1987 Doucette had been convicted of telecommunications fraud in Canada and sentenced to ninety days' imprisonment with two years' probation. She had been charged with running a code line and trafficking stolen access codes. Subsequently, the Canadians reported, Doucette had left the country with her two children.

Later that month an MCI operative, Tom Schutz, told Moore that an informant had passed on the word that a well-known hacker named Kyrie had just moved from the West Coast to the Chicago area. The informant, Schutz said, had overheard the information on a hacker "bridge" (a conference call). At the beginning of April an MCI security officer, Sue Walsh, received information from another informant that Kyrie had a Chicago telephone number.

By mid-month, Moore was able to get court authorization to

attach a dialed-number recorder (DNR), to Doucette's phone. A DNR monitors outgoing calls, recording the number accessed and any codes used. From the surveillance, agents were able to detect a large volume of calls to various voice-mail systems and PBX networks.

The authorities traced the other compromised voice-mail systems to Long Beach, California, and Mobile, Alabama. They discovered that Kyrie was operating code lines on both networks. It's not unusual for hackers to work more than one system; sometimes Hacker A will leave codes for Hacker B on a voice-mail computer in, say, Florida, while Hacker B might leave his messages for Hacker A on a system in New York. By rotating through voice-mail computers in different states, hackers ensure that local law enforcement officials who stumble upon their activities see only part of the picture.

The agents also realized that Kyrie was running a gang. From other sources they heard tapes on which she gave tutorials to neophyte hackers on the techniques of credit card fraud. Over the period of the investigation they identified 152 separate contacts from all over the country, all used as sources for stolen codes. Of the gang, the agents noted seven in particular, whom they identified as "major hackers" within the ring: Little Silence in Los Angeles; the ironically named FBI Agent in Michigan; Outsider, also in Michigan; Stingray from Massachusetts; EG in Columbus, Ohio; Navoronne, also from Columbus; and Game Warden in Georgia.<sup>4</sup> DNRs were also attached to their telephones.

The agents assigned to the case described the group, imaginatively, as "a high-tech street gang." By then the Secret Service had turned the enquiry into a nationwide investigation involving the FBI, the Illinois State Police, the Arizona Attorney General's Office, the Chicago Police Department, the Columbus (Ohio) Police Department, the Cobb County (Georgia) Sheriff's Office, the Royal Canadian Mounted Police, and the Ontario Provincial Police. Security agents from MCI, Sprint, AT&T, and nine Bell phone companies provided technical assistance.

On May 24th the Secret Service asked local authorities in six cities for assistance to mount raids on Doucette's Chicago apartment and the addresses of the five other major hackers in the ring. Prior to the raids the authorities compiled a list of equipment that was to be seized: telephones and speed-dialing devices; computers and peripherals; diskettes; cassette tapes; videotapes; records and documents; computer or data-processing literature; bills, letters, invoices, or any other material relating to occupancy; information pertaining to access device codes; and "degaussing" equipment.<sup>5</sup>

The raid on Doucette's Chicago apartment produced a lode of access codes. Moore found a book listing the numbers for 171 AT&T, ITT, and other telephone cards, as well as authorization codes for 39 PBXs. In addition, the agents found numbers for 118 Visa cards, 150 MasterCard, and 2 American Express cards.

Doucette admitted that she was Kyrie. Later in the Secret Service offices, she confessed to operating code lines, trafficking stolen numbers, and receiving unauthorized Western Union money orders. She was held in custody without bond and indicted on seventeen counts of violating federal computer, access device, and telecom fraud laws between January 1988 and May 1989.

Estimates of the costs of Doucette's activities varied. On the day of her arrest, she was accused of causing "\$200,000 in losses . . . by corporations and telephone service providers." Later it was announced that "substantially more than \$1.6 million in losses were suffered" by credit card companies and telephone carriers.

Doucette's was a high-profile arrest, the first federal prosecution for hacking voice-mail systems and trafficking in access devices. The prosecution was determined that she would be made an example of; her case, the authorities said, would reflect "a new reality for hackers" in the 1990s—the certainty of "meaningful punishment." If convicted of all charges, Doucette faced eighty-nine years' imprisonment, a \$69,000 fine, and \$1.6 million in restitution charges.

The case was plea-bargained. Doucette admitted to one count;

the other charges were dismissed. On August 17, 1990, Doucette, then aged thirty-six, was sentenced to twenty-seven months in prison. It was one of the most severe sentences ever given to a computer hacker in the United States.<sup>6</sup>

Willie Sutton, a U.S. gangster, was once asked why he robbed banks. "Because that's where the money is," he replied.

Little has changed; banks still have the money. Only the means of robbing them have become more numerous. Modern banks are dependent on computer technology, creating new opportunities for fraud and high-tech bank robbery.

Probably the best-known story about modern-day bank fraud involves the computation of "rounded-off" interest payments. A bank employee noticed that the quarterly interest payments on the millions of savings accounts held by the bank were worked out to four decimal points, then rounded up or down. Anything above .0075 of a dollar was rounded up to the next penny and paid to the customer; anything below that was rounded down and kept by the bank. In other words; anything up to three quarters of a cent in earned interest on millions of accounts was going back into the bank's coffers.

Interest earned by bank customers was calculated and credited by computer. So it would be a simple matter for an employee to write a program amending the process: instead of the rounded-down interest going back to the bank, it could all be amalgamated in one account, to which the employee alone had access. Over the two or three years that such a scam was said to have been operational, an employee was supposed to have grossed millions, even billions, of dollars.

The story is an urban legend that has been told for years and accepted by many, but there has not been a single documented case. However, it certainly could be true: banks' dependence on computers has made fraud easier to commit and harder to detect. Computers are impersonal, their procedures faster and more anonymous than paper-based transactions. They can move

# FINANCIAL AFFIDAVIT

CJA 23

IN SUPPORT OF REQUEST FOR ATTORNEY, EXPERT OR OTHER COURT SERVICES WITHOUT PAYMENT OF FEE

IN UNITED STATES  MAGISTRATE  DISTRICT  APPEALS COURT or  OTHER PANEL (Specify below)  
IN THE CASE OF

UNITED STATES vs. DOUCETTE FOR  
NORTHERN DISTRICT  
AT  
CHICAGO, ILLINOIS

LOCATION NUMBER  
ILNCC

DCCKET NUMBERS  
Magistrate  
89 CR 471  
District Court  
Court of Appeals

PERSON REPRESENTED (Show your full name)

LYNNE ~~DOUCETTE~~ **DOCKETED**  
JUN 2 1989

- 1  Defendant—Adult
- 2  Defendant—Juvenile
- 3  Appellant
- 4  Probation Violator
- 5  Parole Violator
- 6  Habeas Petitioner
- 7  2255 Petitioner
- 8  Material Witness
- 9  Other (Specify)

CHARGE/OFFENSE (describe if applicable & check box →)

- Felony
- Misdemeanor

18 USC 1029

**EMPLOYMENT**

Are you now employed?  Yes  No  Am Self Employed  
Name and address of employer: STATE OF ILLINOIS - REHABILITATION SERVICES  
IF YES, how much do you earn per month? \$ 380.00 IF NO, give month and year of last employment  
How much did you earn per month \$ \_\_\_\_\_

If married is your Spouse employed?  Yes  No  
IF YES, how much does your Spouse earn per month \$ \_\_\_\_\_ If a minor under age 21, what is your Parents or Guardian's approximate monthly income \$ \_\_\_\_\_

**ASSETS**

**OTHER INCOME**

Have you received within the past 12 months any income from a business, profession or other form of self-employment, or in the form of rent payments, interest, dividends, retirement or annuity payments, or other sources?  Yes  No  
IF YES, GIVE THE AMOUNT RECEIVED & IDENTIFY THE SOURCES  
RECEIVED 4000.00 SOURCES RAN HOME DAY CARE OR BABY SITTING SERVICE

**CASH**

Have you any cash on hand or money in savings or checking account  Yes  No IF YES, state total amount \$ \_\_\_\_\_

**PROPERTY**

Do you own any real estate, stocks, bonds, notes, automobiles, or other valuable property (excluding ordinary household furnishings and clothing)?  Yes  No

IF YES, GIVE VALUE AND DESCRIBE IT

VALUE	DESCRIPTION
_____	_____
_____	_____
_____	_____

**OBLIGATIONS & DEBTS**

**DEPENDENTS**

- MARITAL STATUS
- SINGLE
  - MARRIED
  - WIDOWED
  - SEPARATED OR
  - DIVORCED

Total No. of Dependents  
2

List persons you actually support and your relationship to them

<u>JEFFREY ADKINS</u>	<u>SON</u>
<u>PATRICK DOUCETTE</u>	<u>SON</u>

**DEBTS & MONTHLY BILLS**

(LIST ALL CREDITORS, INCLUDING BANKS, LOAN COMPANIES, CHARGE ACCOUNTS, ETC.)

Creditors	Total Debt	Monthly Payt.
APARTMENT OR HOME:	\$ _____	\$ _____
_____	\$ _____	\$ _____
_____	\$ _____	\$ _____
_____	\$ _____	\$ _____

I certify the above to be correct.

SIGNATURE OF DEFENDANT  
(OR PERSON REPRESENTED)

Lynne Doucette

5-26-89

**WARNING: A FALSE OR DISHONEST ANSWER TO A QUESTION IN THIS AFFIDAVIT MAY BE PUNISHABLE BY FINE OR IMPRISONMENT, OR BOTH.**

UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

Name of Assigned Judge or Magistrate	LEFKOW		Sitting Judge/Mag. If Other Than Assigned Judge/Mag.	
Case Number	89 CR 471	Date	MAY 26, 1989	
Case Title	U.S.A. v. LESLIE LYNN DOUCETTE			

**MOTION:** [In the following box (a) indicate the party filing the motion, e.g., plaintiff, defendant, 3d-party plaintiff, and (b) state briefly the nature of the motion being presented]


**DOCKET ENTRY:** (The balance of this form is reserved for notations by court staff.)

(1)	<input type="checkbox"/> Judgment is entered as follows:	(2)	<input checked="" type="checkbox"/> [Other docket entry:]
Preliminary examination and detention hearing held. No conditions of bond having been made, defendant is ordered detained as a risk of flight. Order finding of probable cause. Defendant is ordered held to the District Court. Detention order to follow.			
(3)	<input type="checkbox"/>	Filed motion of [use listing in "MOTION" box above].	
(4)	<input type="checkbox"/>	Brief in support of motion due _____.	
(5)	<input type="checkbox"/>	Answer brief to motion due _____ Reply to answer brief due _____.	
(6)	<input type="checkbox"/>	Hearing Ruling on _____ set for _____ at _____.	
(7)	<input type="checkbox"/>	Status hearing <input type="checkbox"/> held <input type="checkbox"/> continued to <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.	
(8)	<input type="checkbox"/>	Pretrial conference <input type="checkbox"/> held <input type="checkbox"/> continued to <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.	
(9)	<input type="checkbox"/>	Trial <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.	
(10)	<input type="checkbox"/>	<input type="checkbox"/> Bench trial <input type="checkbox"/> Jury trial <input type="checkbox"/> Hearing held and continued to _____ at _____.	
(11)	<input type="checkbox"/>	This case is dismissed <input type="checkbox"/> without <input type="checkbox"/> with prejudice and without costs <input type="checkbox"/> by agreement <input type="checkbox"/> pursuant to <input type="checkbox"/> FRCP 4(j) (failure to serve) <input type="checkbox"/> General Rule 21 (want of prosecution) <input type="checkbox"/> FRCP 41(a) (1) <input type="checkbox"/> FRCP 41(a)(2)	
(12)	<input type="checkbox"/>	(For further detail see <input type="checkbox"/> order on the reverse of <input type="checkbox"/> order attached to the original minute order form.)	

X	No notices required.	Date/time received in central Clerk's Office	number of notices	Document #	
	Notices mailed by judge's staff.				JUN 2 1989
	Notified counsel by telephone.				<i>[Signature]</i>
	Docketing to mail notices.				date docketed
Mail AO 450 form.	date mld. notices	docketing dpty. initials	5		
Copy to judge/magistrate.	mailing dpty. initials				
courtroom deputy's initials	<i>[Signature]</i>				



UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

Name of Assigned Judge or Magistrate	LEFKOW	Sitting Judge/Mag. If Other Than Assigned Judge/Mag.	
Case Number	89 CR 471	Date	MAY 25, 1989
Case Title	U.S.A. v. LESLIE LYNN DOUCETTE		

**MOTION:** [In the following box (a) indicate the party filing the motion, e.g., plaintiff, defendant, 3d-party plaintiff, and (b) state briefly the nature of the motion being presented]


**DOCKET ENTRY:** (The balance of this form is reserved for notations by court staff.)

(1) <input type="checkbox"/>	Judgment is entered as follows:	(2) <input checked="" type="checkbox"/>	[Other docket entry:]
Continued initial appearance held. No conditions for bond having been made, the defendant is ordered detained. Preliminary examination and detention hearing set for May 26, 1989 at 3:30.			
(3) <input type="checkbox"/>	Filed motion of [use listing in "MOTION" box above].		
(4) <input type="checkbox"/>	Brief in support of motion due _____.		
(5) <input type="checkbox"/>	Answer brief to motion due _____ Reply to answer brief due _____.		
(6) <input type="checkbox"/>	<input type="checkbox"/> Hearing <input type="checkbox"/> Ruling on _____ set for _____ at _____.		
(7) <input type="checkbox"/>	Status hearing <input type="checkbox"/> held <input type="checkbox"/> continued to <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.		
(8) <input type="checkbox"/>	Pretrial conference <input type="checkbox"/> held <input type="checkbox"/> continued to <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.		
(9) <input type="checkbox"/>	Trial <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.		
(10) <input type="checkbox"/>	<input type="checkbox"/> Bench trial <input type="checkbox"/> Jury trial <input type="checkbox"/> Hearing held and continued to _____ at _____.		
(11) <input type="checkbox"/>	This case is dismissed <input type="checkbox"/> without <input type="checkbox"/> with prejudice and without costs <input type="checkbox"/> by agreement <input type="checkbox"/> pursuant to <input type="checkbox"/> FRCP 4(j) (failure to serve) <input type="checkbox"/> General Rule 21 (want of prosecution) <input type="checkbox"/> FRCP 41(a) (1) <input type="checkbox"/> FRCP 41(a)(2)		
(12) <input type="checkbox"/>	(For further detail see <input type="checkbox"/> order on the reverse of <input type="checkbox"/> order attached to the original minute order form.)		

<input checked="" type="checkbox"/>	No notices required.	Date/time received in central Clerk's Office	number of notices	Document #
	Notices mailed by judge's staff.			
	Notified counsel by telephone.			
	Docketing to mail notices.			
<input type="checkbox"/>	Mail AO 450 form.	JUN 2 1989	date docketed	4
<input type="checkbox"/>	Copy to judge/magistrate.			
<input type="checkbox"/>	courtroom deputy's initials <i>pw</i>	initials	date mld. notices	
<input type="checkbox"/>				initials

UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

Name of Assigned Judge or Magistrate	LEFKOW	Sitting Judge/Mag. If Other Than Assigned Judge/Mag.	
Case Number	89 CR 471	Date	MAY 25, 1989
Case Title	U.S.A. v. LESLIE LYNN DOUCETTE		

MOTION:

In the following box (a) indicate the party filing the motion, e.g., plaintiff, defendant, 3d-party plaintiff, and (b) state briefly the nature of the motion being presented]

<p>Sent for Microfilming JUN 2 1989 Filmed on JUN 7 1989</p>	
--	--

DOCKET ENTRY: (The balance of this form is reserved for notations by court staff.)

(1) <input type="checkbox"/>	Judgment is entered as follows:	(2) <input checked="" type="checkbox"/>	[Other docket entry:]
<p>Initial appearance held. B. Cook assigned AUSA. R. Seeder appointed Federal Defender. Defendant arrested 24 MAY 89. Defendant informed of rights and ordered detained. Continued initial appearance set for 25 MAY 89 at 3:00.</p>			
(3) <input type="checkbox"/>	Filed motion of [use listing in "MOTION" box above].		
(4) <input type="checkbox"/>	Brief in support of motion due _____.		
(5) <input type="checkbox"/>	Answer brief to motion due _____ Reply to answer brief due _____.		
(6) <input type="checkbox"/>	<input type="checkbox"/> Hearing <input type="checkbox"/> Ruling on _____ set for _____ at _____.		
(7) <input type="checkbox"/>	Status hearing <input type="checkbox"/> held <input type="checkbox"/> continued to <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.		
(8) <input type="checkbox"/>	Pretrial conference <input type="checkbox"/> held <input type="checkbox"/> continued to <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.		
(9) <input type="checkbox"/>	Trial <input type="checkbox"/> set for <input type="checkbox"/> reset for _____ at _____.		
(10) <input type="checkbox"/>	<input type="checkbox"/> Bench trial <input type="checkbox"/> Jury trial <input type="checkbox"/> Hearing held and continued to _____ at _____.		
(11) <input type="checkbox"/>	This case is dismissed <input type="checkbox"/> without <input type="checkbox"/> with prejudice and without costs <input type="checkbox"/> by agreement <input type="checkbox"/> pursuant to <input type="checkbox"/> FRCP 4(j) (failure to serve) <input type="checkbox"/> General Rule 21 (want of prosecution) <input type="checkbox"/> FRCP 41(a)(1) <input type="checkbox"/> FRCP 41(a)(2)		
(12) <input checked="" type="checkbox"/>	(For further detail see <input type="checkbox"/> order on the reverse of <input checked="" type="checkbox"/> order attached to the original minute order form.)		

<input checked="" type="checkbox"/> No notices required. <input type="checkbox"/> Notices mailed by judge's staff. <input type="checkbox"/> Notified counsel by telephone. <input type="checkbox"/> Docketing to mail notices. <input type="checkbox"/> Mail AO 450 form. <input type="checkbox"/> Copy to judge/magistrate.	courtroom deputy's initials <i>pw</i>	Date/time received in central Clerk's Office	number of notices	Document # <div style="font-size: 2em; text-align: center;">2</div>	
			JUN 2 1989		date docketed
			<i>ky</i>		docketing dpty. initials
					date mld. notices
			mailing dpty. initials		

United States District Court  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

UNITED STATES OF AMERICA

vs.

LYNN DOUCETTE

)  
)  
)  
)  
)  
)  
)  
)  
)

NO. 89 CV 471

ORDER APPOINTING COUNSEL.

The above-named defendant has testified under oath or has filed with the court an Affidavit of Financial Status and thereby satisfied this court that he or she is financially unable to employ counsel.

Accordingly, the FEDERAL DEFENDER PROGRAM is hereby appointed to represent this defendant in the above designated case unless relieved by an order of this court or by order of the court of appeals.

DATE: 5/25/89

ENTER:

Joan H. [Signature]

Signature of U.S. District Court Judge,  
Magistrate (or Clerk or Deputy Clerk  
by order of the Court)

# United States District Court

DISTRICT

Northern District of Illinois, Eastern Division

UNITED STATES OF AMERICA  
v.

**DOCKETED**

DOCKET NO.

**8900471**

Leslie Lynn Doucette  
a/k/a Kyrie

**JUN 2**

1989  
MAGISTRATE'S CASE NO.

MAGISTRATE

Complaint for violation of Title 18

United States Code § 1029, 1343 and 371

NAME OF JUDGE OR MAGISTRATE

Honorable Joan Humphrey Lefkow

OFFICIAL TITLE

U.S. Magistrate

LOCATION

Northern District of Illinois  
Eastern Division

DATE OF OFFENSE

PLACE OF OFFENSE

ADDRESS OF ACCUSED (if known)

6748-6750 N. Ashland  
Apt. 204  
Chicago, IL.

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

From May, 1988 through May, 1989 the defendant, Leslie Lynn Doucette a/k/a Kyrie, created a scheme to knowingly and with intent to defraud possess more than 15 unauthorized access devices and use one or more unauthorized access devices during a one year period to obtain more than \$1,000.00, in violation of 18 USC 1029(a)(2), 1029(a)(3), 1343 and 371.

FILED-EDS  
89 MAY 24 PM 4:40  
U.S. DISTRICT COURT

BASIS OF COMPLAINANTS CHARGE AGAINST THE ACCUSED:

See the attached affidavit and search warrant affidavit of Special Agent William Conway of the U.S. Secret Service.

MATERIAL WITNESSES IN RELATION TO THIS CHARGE:

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.

SIGNATURE OF COMPLAINANT (official title)

OFFICIAL TITLE

*William Conway*  
Special Agent USSS

Sworn to before me and subscribed in my presence,

SIGNATURE OF MAGISTRATE(1)

DATE

7 MAY 25 1989

*Joan H. Lefkow*

1) See Federal Rules of Criminal Procedure rules 3 and 54.

STATE OF ILLINOIS )  
 ) SS  
COUNTY OF COOK )

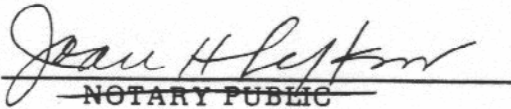
AFFIDAVIT

1. Your affiant has been a Special Agent of the U.S. Secret Service for seven years and has been an agent of the U.S. Treasury Department for thirteen years. I am submitting this affidavit in support of the arrest of Leslie Lynn Doucette.
2. As a result of information provided to MCI security April, 1989 and to protect its customers MCI attached a dialed number recorder to telephone line 312-262-7217. On April 30, 1989 and May 1, 1989 the DNR picked up outgoing telephone calls ~~from~~<sup>to</sup> number which checked the validity of more than 15 access devices, specifically 23 Master Card credit cards and 6 Citicorp Visa credit cards.
3. On May 24, 1989 Doucette admitted operating a scheme whereby unauthorized credit card numbers were used to obtain money through Western Union. Doucette stated that she obtained credit card numbers from various voice mail computer systems and hackers over the past year. She and other individuals working with her would then check the validity of the credit card numbers by calling various credit card validation computers. She gave valid credit card numbers to hackers with the agreement that they would use the credit cards to purchase Western Union money orders payable to her. The hackers would then contact Western Union and request money orders payable to her through an alias she would designate, which were then paid for by the unauthorized credit card numbers. Doucette said she received around \$1,000 in the past year through the use of this scheme.
4. On 5/24/89 the search warrant attached to this complaint was executed against Apt. 204 of 6748-6750 North Asland in Chicago, Illinois. At the time the warrant was executed the defendant Lynn Doucette was present and acknowledged that she uses the name Kyrie. The telephone number in the apartment was 312-262-7217.

5. At the time of the search agents found a series of books with credit card codes, telephone access codes and telephone calling card numbers. One book alone contained 71 AT&T calling card numbers, 31 Visa, American Express, and Master Card numbers, 24 calling card numbers, including MCI, Sprint, ITT, 32 PBX numbers, 42 Loops (conference call numbers), and 24 Diverters.

  
AFFIANT

SUBSCRIBED and SWORN to Before  
me this 24th day of May, 1989

  
NOTARY PUBLIC

WJC/lg B/7

AF FIDAVIT FOR SEARCH WARRANT

AUSA William Cook  
U.S. Atty. Off. 312-353-760

<p align="center"><b>United States District Court</b></p>	<p>DISTRICT Northern District of Illinois Eastern Division</p>	
<p align="center">United States of America vs. Apartment 204 at 6748-6750 North Ashland Street in Chicago, Illinois and any other area physically connected to telephone line (312) 262-7217</p>	<p>DOCKET NO.</p>	<p>MAGISTRATE'S CASE NO.</p>
<p>NAME AND ADDRESS OF JUDGE<sup>1</sup> OR FEDERAL MAGISTRATE</p>		

The undersigned being duly sworn deposes and says: That he/she has reason to believe that

on the person of     on the premises known as

DISTRICT  
Northern District of Illinois, Eastern Division

Apartment 204 located in the multi-story apartment building located at 6748-6750 North Ashland Street in Chicago, Illinois and any other area physically connected to the telephone line (312) 262-7217. (See Attachment 1, photographs of the exterior of 6748-6750 North Ashland, Chicago, Illinois.)

The following property is concealed:

Telephones with speed dialing and memory and the memory contained in said equipment; computing and/or data processing device(s) and associated peripheral equipment and memory contained in said equipment; records, notes, logs and journals; indicia of occupancy of the residence and indicia of use of the telephone and computer equipment and other materials further specified and defined in Attachment 2 to the Affidavit.

Affiant alleges the following grounds for search and seizure<sup>2</sup>

The above described property (including the property in Attachment 2 to this Affidavit) constitutes evidence, instrumentalities and fruits of the crimes of possession of and trafficking in unauthorized access devices (18 U.S.C. §1029); accessing a federal interest computer with intent to defraud (18 U.S.C. §1030(a)(4)); trafficking in computer access information (18 U.S.C. §1030(a)(6)); unlawfully accessing electrically stored communications, (18 U.S.C. §2701(a)(1); wire fraud (18 U.S.C. §1343); interstate transportation of fraudulently obtained property (18 U.S.C. §2314); conspiracy (18 U.S.C. §371); and the commission of two or more acts of racketeering (18 U.S.C. §1962 and 1963).

See attached affidavit which is incorporated as part of this affidavit for search warrant

Affiant states the following facts establishing the foregoing grounds for issuance of a Search Warrant

See attached affidavit of S.A. William P. Conway which is incorporated as part of this affidavit.

SIGNATURE OF AFFIANT	OFFICIAL TITLE, IF ANY
----------------------	------------------------

Sworn to before me, and subscribed in my presence:

DATE	JUDGE <sup>1</sup> OR FEDERAL MAGISTRATE
------	--

<sup>1</sup>United States Judge or Judge of a State Court of Record.  
<sup>2</sup>If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure 41(c), show reasonable cause therefor.

STATE OF ILLINOIS )  
                          )     SS  
COUNTY OF COOK    )

AFFIDAVIT

1. Your affiant has been a Special Agent of the U.S. Secret Service for seven years and has been an agent of the U.S. Treasury Department for thirteen years. I am submitting this affidavit in support of an application for a Search Warrant for Apartment 204 and any other area physically connected to telephone line 312-262-7217 in the apartment building at 6748-6750 North Ashland, Chicago, Illinois, which apartment is listed to Dawn L. Petty. The information contained herein (unless otherwise noted) is based on my personal observations as well as information supplied to me by other agents of the U.S. Secret Service, the FBI, the Illinois State Police (ISP), the Arizona Attorney General's Office, the Columbus Ohio Police Department, the Royal Canadian Mounted Police and by other law enforcement agents; and officials in the security and technical sections of telecommunications companies including MCI, Sprint, AT&T, Illinois Bell, Pacific Bell, Michigan Bell, Ohio Bell, Southern Bell, Southwestern Bell, New England Bell, Bellcore and Canadian Bell.

2. Your affiant has also received technical information and investigative assistance from the following experts in the field of telecommunication fraud and computer fraud investigations:

A. Sgt. Abigail Abraham, ISP-DCI has been employed by ISP-DCI for eight and half years and has been employed full time as the head of ISP-DCI computer and telecommunications fraud investigation unit for the past three years. During this three year period she has executed 20 to 25 search warrants in telecommunication and computer fraud investigations generally and has conducted five separate investigations involving voice mail computer fraud allegations. Sgt. Abraham is an instructor at the Federal Law



Enforcement Training Center in Glencoe, Georgia on telecommunications fraud investigations.

b. Detective Robert Synder has been with the Columbus Ohio Police Department for fifteen years and has actively investigated telecommunications fraud cases for the past six years. He has conducted sixteen separate telecommunication and computer fraud investigations during this period and executed eight telecommunications fraud warrants, three of which have specifically involved voice mail computer fraud allegations. Detective Synder also has instructed federal agents at the Federal Law Enforcement Training Center and the Institute of Police Training and Management.

c. Tom Schutz, MCI Security Director for the Chicago area has been employed investigating telecommunications fraud for the past six years, during which time he has investigated approximately 137 computer hacker cases and participated in approximately 92 to 93 search warrants in telecommunication fraud cases. He has maintained his expertise in the telecommunications industry by frequent attendance at telecommunication security conferences throughout the United States. Prior to being employed by MCI, Schutz was employed for over four years with the Chicago Police Department.

3. Your affiant has also received substantial information from S.A. William "Fred" Moore of the U.S. Secret Service - Chicago, who has been with the Secret Service for eighteen and <sup>one-</sup> half years and is presently assigned to the Fraud Section of the U.S. Secret Service in Chicago. S.A. Moore is the case agent assigned to the investigation of the fraud against Source 1 (described below) and the follow-up investigation of the hackers who have attacked Source 1 and other voice mail computer systems throughout the United States and Canada.

## Overview of Investigation

4. My investigation and investigation by S.A. Moore (United States Secret Service - Chicago) and by other Special Agents of the U.S. Secret Service and other law enforcement agencies described in this affidavit has disclosed that as many as 50 computer "hackers" using various code names or "handles" are involved in a nationwide conspiracy to steal telephone and computer service from voice mail computers operated by certain victim companies and organizations and to illegally traffic and market commercial credit card numbers (Visa, Mastercard, American Express, etc.) and telephone calling card numbers (AT&T, MCI, Sprint, etc.) on these victim company's voice mail computers. Information regarding this conspiracy was first received by the U.S. Secret Service in Chicago in February, 1989 and investigation to date has established that substantially more than \$200,000.00 in losses has been suffered by the victim companies and telephone service companies as a result of the conspiracy.

5. S.A. William Fred Moore, (United States Secret Service - Chicago) has advised me that while as many as 50 computer "hackers" (hackers are defined as individuals involved with the unauthorized access of computer systems by various means) are involved in the conspiracy at any one time, eight principal computer hackers at the following locations form the hub or core group of the conspiracy.

"Handle"

Telephone Location

Kyrie

Lynn Doucett  
c/o Dawn Petty  
6748 N. Ashland, Apartment 204  
Chicago, IL  
Telephone: 312-262-7217  
Also uses: 205-341-8006  
And before May 1989: 205-341-8448

Little Silence

Luis J. Aguilar (Ester Aguilar)  
6302 Hereford Drive  
Los Angeles, California  
Telephone: 213-726-4012/728-6967/728-6199  
Also uses: Velayo Voice Mail Service  
1-800-888-5359

<b>FBI Agent</b>	<b>Phillip T. Colley</b> 14338 Pernel Drive Sterling Heights, Michigan Telephone: 313-247-9252
<b>Outsider</b>	<b>William Gotts</b> 37140 Camelot Drive (As of March, 1989) Sterling Heights, Michigan Telephone: 313-826-8659
<b>Stingray</b>	<b>Paul J. McMahon</b> 141 Waverly Avenue Melrose, MA Telephone: 617-662-7939 (bbs) 617-665-7822
<b>Navoronne Group</b> Ed Grimley	<b>c/o Carol Schwartz</b> 5893 Effingham Road Columbus, Ohio Telephone: 614-225-2450
<b>Navoronne Group</b>	<b>Mark Mastenbrook</b> 5592 Bairsford Cir. N. Columbus, Ohio Telephone: 614-861-4327
<b>Game Warden</b>	<b>John Vouidy</b> 1722 Thorrs Rokk N.E. Marietta, Georgia Telephone: 404-642-1987

6. S.A. Moore advises me that the above named individuals may not necessarily be the violators in the case. They may merely be the individuals named as the telephone service subscriber at the location being used by the violator.

Statutes Involved

7. 18 U.S.C. 1343 prohibits the use of interstate wire communications as part of a scheme to defraud, which includes obtaining money or property (tangible or intangible) by a criminal or the loss of something of value by the victim. Investigation by your affiant has determined that the actions of the computer hackers involved here initially defrauded the victim companies by fraudulently increasing their monthly payments for telephone services and causing

them to incur substantial expense to secure their voice mail computer systems from further attack. Losses from this aspect of the scheme to the companies operating the VM computer are known to be in excess of \$200,000.00. A secondary fraud by the hackers operated against credit card companies and telephone companies whose access codes were exchanged on the VM computers. Conversely, the computer hackers gained valuable property because their fraud scheme provided them with telephone access codes and financial institution access codes which in turn could be used by them to obtain telephone services and property which was charged to the victim companies. Their scheme also provided them access to private business exchange (PBX) numbers which could be used to obtain telephone service which was charged to the victim companies. Finally, the scheme provided the hackers with computer access codes to enter and use interstate computer networks.

8. 18 U.S.C. 1030 prohibits unauthorized access to a Federal Interest computer with intent to defraud. Intent to defraud has the same meaning as in the wire fraud statute. A Federal Interest computer is defined as "one of two or more computers used in committing the offense, not all of which are located in the same state." 18 USC 1030(e)(2). Investigation here has established that Federal Interest computers are involved in that the fraud scheme involved the abuse of voice mail computers in Illinois, California, Florida, Washington and Virginia by computer hackers in Illinois, California, Michigan, Ohio, Georgia and Massachusetts. Moreover, Robert Gates of Ameritech has advised S.A. Moore (United States Secret Service - Chicago) that the interstate access to the Illinois victim's voice mail (VM) computer could only be gained through the use of an electronic switching signal (ESS) computer in the state where the hacker originated the call. Thus, telephone calls made from California, Ohio, Georgia, Massachusetts and Michigan used the ESS computer in each of those states and in Illinois to

gain access to the VM computer in Illinois.

9. 18 U.S.C. 1029 prohibits the unauthorized possession of 15 or more unauthorized or counterfeit "access devices" with intent to defraud and trafficking in unauthorized access devices with an intent to defraud and an accompanying \$1,000.00 profit to the violator or loss to the victim. These prohibitions also apply to members of a conspiracy to commit these offenses. Intent to defraud has the same meaning as in the wire fraud statute. "Access devices" include credit cards issued by various companies and long distance telephone access codes. An "unauthorized access device" is any access device obtained with intent to defraud. Investigation here has established that over 130 unauthorized or counterfeited access devices were trafficked on Source 1's voice mail computer in February and March, 1989 by various conspirators and that victim companies were defrauded out of more than \$200,000.00 in telephone services.

10. 18 U.S.C. 2701 prohibits unlawfully accessing a facility containing electrically stored communications. The investigation here has established that companies using voice mail computers are facilities containing electrically stored information. Access to these computers without authorization by the computer hackers in this case violated this law.

11. Other federal statutes violated here are familiar to the Court. 18 U.S.C. 2314 prohibits the interstate transportation of fraudulently obtained property. 18 U.S.C. 1962 and 1963 prohibit the commission of two or more acts of racketeering (including two or more acts violating 18 U.S.C. 1343 and/or 2314,) and including forfeiture of instrumentalities used or obtained during the execution of a crime). 18 U.S.C. §371 is the federal conspiracy law.

#### Evidence That a Crime Has Been Committed

12. On or about February 9, 1989, Special Agent Mike Cleary, Agent In-Charge of the Fraud Unit (U.S. Secret Service Chicago) was contacted by a

Rolling Meadows, Illinois real estate company, operated by Source 1. (See sealed Affidavit.) Source 1 reported that he had discovered that his company's voice mail computer system was being attacked by computer hackers. S.A. Cleary advised Source 1 that he would have Secret Service agents visit him on within a few days.

13. On February 15, 1989 Special Agent Moore and Special Agent Bill Tebbe (United States Secret Service - Chicago) went to the Rolling Meadows real estate company and met Source 1. Source 1 advised that in the Fall of 1988 his company had installed a GENISIS voice mail computer system (VM computer) to better service their customers and employees. Computer mail box numbers and mail box entry codes were personally established, authorized and assigned on the VM computer by Source 1.

14. Source 1 explained that his VM computer system allows authorized individuals to use a "voice mailbox" which is capable of performing several functions. The computer has the ability to receive and store messages from callers, to send messages to other boxes on the system, and to send messages to a pre-selected group of other voice mail boxes. These functions are achieved by the caller pushing the appropriate numerical commands on a telephone keypad for the desired function. To leave a message on the VM computer the caller dials the company's "800" number, and the computer answers with a message identifying the system as the voice mail service of the company. The caller is then instructed to enter the number of the box he wishes to reach. The caller enters a four-digit number, and hears whatever greeting the box owner has chosen to leave. The caller can exercise several options, one of which is to leave a message after the tone. In this respect, the voice-mail system operates much like a telephone answering machine. Rather than being recorded on audio tape, however, the message is stored in digitized form by the computer system. The entire voice-message system is actually a computer system accessible through telephone lines. The

messages are stored on large-capacity computer disks.

15. Source 1 states that an outside caller needs to know only the assigned box number in order to leave a message for an individual or employee. In order to retrieve the messages or to delete them from the system, however, the person to whom the box is assigned must have both the box number and a confidential password — the password ensures privacy of the communications by acting as a "key" to "unlock" the box and reveal its contents. The employee to whom the box has been assigned also has the ability to change his password, thereby preventing access to the box contents by anyone who may have learned his password.

16. While the "800" number or general number of a company's VM computer is published, the access codes to individual voice mail boxes are not disclosed to anyone but the authorized user and the computer's systems administrator, according to Source 1.

17. Source 1 further advised that in about November 1988, during a routine review of messages on the VM computer, he noticed that unauthorized computer hackers had begun leaving messages in the VM computer. He advised that initially the intrusions on the VM computer appeared to be infrequent. However, by December, 1988 the volume of hacker intrusions increased and by January, 1989 the hacker attacks became so frequent that sometimes they virtually "took over" the VM computer by changing the passwords to deny access to the assigned users and the systems administrator, Source 1.

18. Source 1 advised Special Agent Moore and Special Agent Tebbe that a significant increase in the use of the VM computer and the company's telephone bills had occurred as a result of the hacker activity. While he did not yet know the full extent of financial losses, he advised that his company pays MCI for each call into their "800" number which is answered by the VM computer. (In late March, 1989 Source 1 stated that his estimated loss figure due to unauthorized use of

his VM computer exceed \$1,600.00). Source 1 further advised that by February, 1989 the hackers have occupied a significant portion of the VM computer's available disk storage capacity and caused him to incur expenses as he attempted to secure the computer.

#### Identification of Hackers

19. In February and March, 1989 Source 1 authorized Special Agent Moore and other agents of the United States Secret Service to make consensual recordings of the messages that had been left by the hackers on his VM computer system. Thereafter, on seven dates in early March, 1989 Special Agent Moore, Special Agent Pingolt and other Secret Service Agents tape recorded the unauthorized messages on the Rolling Meadows company's VM computer system with the consent of Source 1.

20. Special Agent Moore has advised your affiant that MCI provides the "800" line that provides telephone access to Source 1's VM computer. MCI has automatic number identification on the VM computer line which gives MCI the capacity to identify the source of incoming calls to Source 1's "800" number. Special Agent Moore obtained the MCI computer printouts of calls coming into Source 1's "800" number between December, 1988 and the end of March, 1989 from Tom Schutz, MCI Security Chicago, and observed high volumes of calls originating from several out-of-state callers. Special Agent Moore then obtained subscriber information from law enforcement officials and telephone company security officials on the telephone numbers listed below. A summary of those telephone calls from March 1 to March 27 is presented below.

<u>Subscriber State</u>	<u>Telephone #</u>	<u>3/89</u>
Aguilar (CA)	213-726-4012	332
Colley (MI)	313-247-9252	135
Gotts (MI)	313-826-8659	66
McMahon (MA)	617-662-7939	17
Schwartz (OH)	614-861-2450	104
Mastenbrook (OH)	614-861-4327	12
Voudy (GA)	404-642-1987	51



21. By comparing the date and time of the calls to the "800" number on the MCI billing information with the date and time of the calls automatically recorded after the various messages were left on the VM computer, Special Agent Moore was able to establish that the telephone hackers using the following handles were located at the indicated addresses and were using the below listed telephones.

<u>Handle</u>		<u>True Name/Location</u>	<u>Telephone</u>
FBI Agent	is at	Phillip T. Colley 4338 Pernel Drive Sterling Heights, MI	313-247-9252
Outsider	is at	William Gotts 37140 Camelot Drive Sterling Heights, MI	313-826-8659
Wish Doctor	is at	Athanasios Filias 33060 Richardo Drive Sterling Heights, MI	313-264-8121
		Mark Mastenbrook 5592 Bairsford Circle North Columbus, OH	614-861-4327
Ed Grimley	is at	c/o Carol Schwartz 5893 Effingham Road Columbus, OH	614-861-2450
Stingray	is at	Paul J. McMahon 141 Waverly Avenue Melrose, MA	617-662-7939 (bbs) 617-665-7822
Little Silence	is at	Luis J. Aguilar (Ester Aguilar) 6302 Hereford Drive Los Angeles, CA	213-726-401 213-728-6967 213-728-6199
		John Vouidy 1722 Thorrs Rokk, N.E. Marietta, GA	404-642-1987

22. One of the other hackers using Source 1's VM computer has been identified by Gail J. Thackery of the Arizona Attorney General's Office, S.A. William Conway (U.S. Secret Service - Chicago) and Tom Schutz (MCI Security Chicago) as follows:

Handle

True Name & Address

Kyrie

Lynn Doucett  
c/o Dawn Petty  
6748 N. Ashland, Apartment 204  
Chicago, IL  
Telephone: 312-262-7217  
Also uses: 205-341-8006  
And before May 1988: 205-341-8448

23. Special Agent Moore advised your affiant that he contacted Source 1 with respect to the above telephone numbers and subscribers (Paragraphs 20, 21 and 22) and Source 1 advised that none of the telephones or the listed subscribers were authorized users of his company's VM computer or any of the "mail boxes" on the computer system.

24. Special Agent Moore then caused a summary of the tape recording of the hacker traffic on Source 1's voice mail computer to be prepared by the Secret Service Chicago. That summary reflects that between February 10, 1989 and March 20, 1989 hackers exchanged approximately 130 unauthorized or counterfeited access devices on Source 1's VM computer including 107 long distance telephone access card numbers and 21 bank and corporate credit card numbers (Visa, Mastercharge, American Express and Discover cards) and 2 computer network access numbers. These card numbers are access devices under the definition of "access device" in 18 U.S.C. 1029(e)(1).

25. Special Agent Moore has contacted the long distance carriers involved with the 107 long distance telephone access card numbers and has been advised that none of the individuals named below (nor anyone at the indicated address) was an authorized user of their long distance telephone access card numbers during the period February 10, 1989 to March 20, 1989:

Phillip T. Colley  
4338 Pernel Drive  
Sterling Heights, MI

Luis J. Aguilar  
6302 Hereford Drive  
Los Angeles, CA

Lynn Doucett  
c/o Dawn Petty  
6748 N. Ashland, Apartment 204  
Chicago, IL

Carol Schwartz  
5893 Effingham Road  
Columbus, OH

William Gotts  
37140 Camelot Drive  
Sterling Heights, MI

Mark Mastenbrook  
5592 Bairsford Circle North  
Columbus, OH

Anthanasios Filas  
33060 Richardo Drive  
Sterling Heights, MI

Paul J. McMahon  
141 Waverly Avenue  
Melrose, MA

John Voudy  
1722 Thorrs Rokk, N.E.  
Marietta, GA

26. Special Agent Moore's examination of the unauthorized traffic on Source 1's VM computer also disclosed that 43 other 800 #'s were being trafficked by hackers on Source 1's VM computer including "800" #'s for the following companies:

Proxy Message Center  
Brisbane, California

Arlington County Government Center  
Arlington, Virginia

Kinko Copies Corp.  
Ventura, California

Technology Unlimited  
Seattle, Washington

Miami Voice Mail  
Miami, Florida

27. Contact with these companies by Special Agent Moore and other agents of the Secret Service and the FBI established that each of these companies had also had its voice mail computers "hacked" into by intruders within the past four months. They further advised that the hackers had used their VM computers to exchange credit card codes and that their telephone service charges as a result were substantial. One of the companies had to pay over \$100,000.00 in fraudulent telephone service charges.

28. Sargeant Abigail Abraham of the Illinois State Police has reviewed

the schedules and summaries prepared by Special Agent Moore and states that, based upon her experience investigating voice mail computer cases, the hackers using the VM computer of Source 1 are using Source 1's voice mail computer to exchange information including credit card numbers and ID's, telephone access codes, computer access codes, PBX access codes and access numbers for other voice mail computers. Sargeant Abraham further states that traffic from one individual hacker to another is not limited to one voice mail box and that in fact her experience is that after a hacker enters the architecture of the voice mail system the hacker routinely moves from one coded mail box to another picking up the traffic left in that mail box and leaving new access codes and messages in those boxes. Sargeant Abraham states that the summaries prepared under the direction of your affiant clearly show this traffic pattern between the hackers named above in paragraph 21.

29. Special Agent Moore's investigation of the attack on Source 1's VM computer reflects that one of the hackers soliciting access codes on Source 1's VM computer used the handle Kyrie and Associates.

#### Examination of Individual Hackers

##### A. Doucett

30. Special Agent Moore advises that Tom Schutz (MCI - Chicago) states that on March 24, 1989 he was advised by a reliable informant that a well known hacker named Lynn Doucett (handle "Kyrie") had just moved from the west coast to the Chicago area. Schutz's informant states that this information about Kyrie was overheard by the informant on a "bridge" (a bridge is a telephone hacker expression for a conference call among several hackers.) Schutz advised Special Agent Moore that the informant has provided information in prior investigations that has been independently corroborated.

31. Subsequently, on April 3, 1989, Schutz was advised by MCI Corporate Security in Denver, Colorado that another MCI Security Officer named Sue Welsh had received information from a reliable informant that Lynn Doucett a/k/a Kyrie

had a Chicago contact number of (312) 262-7217.

32. Schutz ordered a subscriber location check on (312) 262-7217 from Illinois Bell Telephone (IBT) and was advised that bills for telephone number (312) 262-7217 were being sent to an address on West Pratt Street in Chicago. However, a subsequent line check by IBT determined that (312) 262-7217 was in fact located at 6748 North Ashland, Apartment 204, in Chicago, Illinois and registered to an individual named Dawn Petty.

33. Investigation by Sargeant Abigail Abraham, Illinois State Police, with the Illinois Department of Public Aid determined that while Dawn Petty was a single person her recent filings with the Illinois Department of Public Aid reflected that 3 other people were living with her in Apartment 204 at 6748 North Ashland.

34. Schutz contacted Canadian Bell Telephone Security and was advised that Lynn Doucett a/k/a Kyrie is the mother of two children ~~that~~<sup>who</sup> travel with her. Doucett is further described as a white female, 35 years old. Canadian Bell officials advise that two years ago Doucett was convicted of telecommunications fraud in Canada and left that country with her two children. Canadian Bell officials advised Schutz that Doucett a/k/a Kyrie has no visible means of support and that she supports herself and her children with her "hacking" activities which include using stolen or counterfeit credit card numbers from various hackers and then obtaining money orders or cash by using the credit card numbers. She then directs other hackers to pick-up the money orders purchased in this manner and mail the money to her. Schutz advised that information from Canadian Bell and other MCI security officials indicated that Doucett a/k/a Kyrie had been an active hacker continuously for at least the last 6 to 7 years.

35. On April 14, 1989, to protect MCI's telephone network and its customers, Schutz ordered the installation of a pen register (also known as a dialled number recorder or DNR) on the telephone (312) 262-7217. On April 19, 1989 the DNR

was installed and Schutz immediately observed a large volume of illegal telephone hacking from that telephone number including the apparently unauthorized use of numerous voice mail computer systems, long distance calling codes and corporation PBX networks to test the validity numerous credit numbers and telephone access codes.

36. Schutz states that as of May 22, 1989 the user at telephone number (312) 282-7217 is still actively involved in the above activity and is using telephone "bridges" (conferences). Based upon his experience, Schutz is aware that these "bridges" are frequently used by hackers for conference to exchange information and access codes.

37. On May 15, 1989 Special Agent Moore received a copy of a transcript of a telephone conference between Kyrie and other hackers on December 11, 1988. The transcript show Kyrie conducting a tutorial for hacker Raymond Bishop on how to fraudulently obtain personal identification numbers from individuals with AT&T calling cards. This transcript was prepared under the direction of Assistant Attorney General Gail Thackeray (Arizona Attorney General) and is based upon a cassette tape seized during the execution of a search warrant against Bishop's residence in February, 1989. During the course of the investigation on Bishop Thackeray had occasion<sup>1</sup> to listen to tapes in which she heard Kyrie's voice. Thackeray was able to identify Kyrie through investigation, information from co-conspirators and/or subsequent conversation with Kyrie in which she (Kyrie) so identifies herself.

38. Assistant Attorney General Thackeray<sup>2</sup> also advised Special Agent Moore (United States Secret Service - Chicago) that on May 1, 1989 Kyrie called her at the Arizona Attorney General's office in Phoenix. During this conversation Kyrie stated that she had numerous hacker identification records and at one point Assistant Attorney General Thackeray<sup>3</sup> heard what sounded like pages in a book turning while Kyrie said she was looking up information about a "hacker."

39. On May 11, 1989 at 7:45 p.m. Special Agent Paul Morrissey of the United States Secret Service - Chicago received a telephone call from two males who identified themselves as Jim or Tim LNU and FNU Feener or Freway and said

they were "phone people." They said that a white female, who had allegedly been convicted of a felony in Canada, was illegally using credit card codes and "burning up the telephone lines." They stated that this woman resides somewhere in Chicago at telephone number 312-262-7217.

40. On May 15, 1989 Special Agent William Conway (United States Secret Service - Chicago) received a certified copy of the criminal record and fingerprints of Leslie Lynn Doucette from the Criminal History Branch of the Royal Canadian Mounted Police (RCMP). The RCMP records reflect that on March 12, 1987 Leslie Lynn Doucette was convicted of telecommunications theft in Canada and sentenced to 90 days in custody and two years probation. RCMP records reflect that Doucette was born April 20, 1954.

Aguilar

41. Special Agent Moore's investigation determined that 332 unauthorized telephone calls to Source 1's VM computer were made in March, 1989 from telephone number 213-726-4012 subscribed to by Luis Aguilar, 6302 Hereford Drive, Los Angeles, California. As part of this investigation a court ordered pen register (DNR) was obtained for the above telephone number on April 17, 1989. Review of the DNR tapes on the Aguilar residence by Special Agent Moore disclosed that between April 17, and May 20, 1989 sixty (60) different telephone "800" numbers were called from the Aguilar telephone to VM computers at various other victim organizations and companies including the following:

ARLINGTON COUNTY GOVERNMENT CENTER VMS  
CYBERLINK VOICE MESSAGING VMS  
RCA TELEPHONE SYSTEM SALES VMS  
HOME BOX OFFICE VMS  
BAKER AND TAYLOR VMS  
GRACE TECHNICAL GROUP VMS  
ASPEN AUTOMATED ANSWERING SYSTEM VMS  
STRATACOM AFTER HOURS ATTENDENT VMS  
ALLIANCE TELECONFERENCING  
I. B. DEFUSSION  
VECTOR DEVELOPMENT VMS  
H.P. PRODUCTS VMS

42. Your affiant has contacted the above referred to companies and learned that they have no authorized anyone named Aguilar at telephone number 213-726-4012 to use their voice mail computer system and that they regard telephone calls from that number to be unauthorized access to their system.

43. Further examination of the DNR on the Aguilar residence disclosed that the Aguilar hacker was transmitting 2600 HZ tones into the telephone receiver in an effort to obtain unauthorized free telephone service through the use of either a "blue box" or a "blue box" simulator computer program. A blue box, or a blue box simulator, is a device that generates 2600 Hertz for use in obtaining free, unauthorized telephone service. Transmission of 2600 Hertz across the telephone network under same circumstances triggers the telephone network to create no billing record of the telephone call. The tone has no legitimate use on a telephone network other than by authorized telephone company employees during the commission of their business.

44. On April 3, 1989 Special Agent Robert Davidson (U. S. Secret Service - San Francisco) was advised by Howard Hubbell of Proxy Voice Message Center NEAR San Francisco (1-800-228-6423) that since March 3, 1989 the Proxy VM computer had been besieged by hackers intent on distributing codes for credit cards (U.S. Sprint, MCI, etc.) and PCP the computer network on Proxy's VM computer. One male hacker with a Spanish accent learned the computer's administrative password and left an extortion message for Hubbell on the VM computer system that if Hubbell did not give the hacker his own voice mailbox then the hacker would continue to hack the system and start leaving messages on mailboxes used by Proxy's customers. On March 31, 1989 Hubbell left a message for the hacker that he needed time to talk to his manager about giving the hacker a voice mail box. However, during the evening of March 31, 1989 the hacker used the computer's administrative password and completely shut out Proxy and its customers and effectively took over the company's VM computer. Hubbell said he was lucky to get the password code back from the hacker without having the vendor conduct a database search. Tapes of hacker activities on Proxy's VM computer were given to the Secret Service and Pacific Bell in mid-April, 1989.

45. S.A. Moore (U. S. Secret Service - Chicago) has advised your affiant that he has listened to telephone recordings of Aguilar from telephone number



213-726-4012 on Source 1's VM computer system and listened to recordings of the unauthorized hacker on the Proxy VM computer in the San Francisco area and states that they are the same person. S. A. Moore further states that the same person's voice was also heard by him on the introduction to the Velayo VMB (800-888-5359).

46. Mark Yelchak, Pacific Bell Corporate Security has also listened to the hacker on the Proxy VM computer tapes and the voice on the Velayo VMB (800-888-5359) and states that they are the same person.

Colley

47. S.A. Moore's investigation determined that 135 unauthorized telephone calls were made to Source 1's VM computer in March, 1989 from telephone number 313-247-9252 listed to Phillip Colley in Sterling Heights, Michigan. As part of this investigation a court ordered pen register (DNR) was obtained for the above telephone number on April 6, 1989.

48. Examination by Special Agent Bruce Towers (United States Secret Service - Detroit) of the DNR on the Colley residence in Sterling, Michigan from April 19, 1989 to May 10, 1989 disclosed that a hacker at that telephone (313-247-9252) was accessing 11 different 800 numbers including the following:

The Michigan Department of Treasury  
VMS  
Dee Kay Enterprises  
Birmingham, Michigan

Further examination of the DNR disclosed that the Colley hacker was transmitting 2600 HZ tones into the telephone receiver in an effort to obtain free telephone service through the <sup>unauthorized</sup> use of either a "blue box" or a "blue box" simulator computer program.

McMahon

49. S.A. Moore's investigation determined that 17 unauthorized telephone calls were made to Source 1's VM computer in March, 1989 from telephone number 617-662-7939 listed to Paul J. McMahon, 141 Waverly Avenue, Melrose, Massachusetts. As part of this investigation a court ordered pen register (DNR)

was obtained for the above telephone number on May 10, 1989. Examination of the DNR on the McMahon residence in Melrose, Massachusetts from May 1, 1989 to May 20, 1989 disclosed that a hacker at telephone number (617-662-7939) was accessing different "800" numbers.

50. Taped conversations of Source 1's VM computer indicated that a hacker named Paul at 617-662-7939, using the "handle" Stingray of the BFI group was taking access codes from the VM computer and posting them on his computer bulletin board (617-665-7822).

51. In April, 1989 Russ Silva of New England Bell Corporate Security attempted to gain access to the alleged computer bulletin board run by "Stingray." Silva confirmed that 617-665-7822 did in fact carry a computer bulletin board. However, Silva was denied access to the board by the system administrator.

Voudy

52. Special Agent Moore (United States Secret Service - Chicago) determined that 51 unauthorized telephone calls to Source 1's VM computer were made from telephone number 404-642-1987 listed to John Voudy in Marietta, Georgia. As part of this investigation a court ordered pen register (DNR) was obtained for the Voudy telephone number on April 19, 1989.

53. Examination by Special Agent William Gleason (United States Secret Service - Atlanta) of the DNR on the Voudy residence in Marietta, Georgia from April 19, 1989 to May 20, 1989 disclosed that a hacker at that telephone number (404-594-9892) was accessing 17 different "800" numbers including:

KINKO COPIES CORP. VMS  
REPUBLIC TELECOMMUNICATIONS  
TMC OF ORLANDO VMS  
I.B. DEFUSSION VMS

54. The Security Officer at Kinko Copies Corp. authorized Special Agent William M. Gleason (United States Secret Service - Atlanta) to consensually record an unauthorized message placed on their VM computer system by the hacker from the Voudy phone. That message disclosed that the Voudy hacker (using the handle Game Warden) was posting AT&T calling cards and 800 numbers of the Kinko VM system for other hackers to use. The hacker was also promising to post access codes, such as VISA credit card numbers, in the future.

55. Examination of DNR records in Columbus, Ohio by Detective Bob Synder

on May 17, 1989 disclosed that telephone calls are going from the Columbus hacker's telephone (614-698-2446) to the Voudy telephone in Marietta.

56. Special Agent Moore (United States Secret Service - Chicago) has contacted the above referred to companies and learned that they have not authorized anyone named Voudy at telephone number 404-642-1987 to use their VM computer system and they regard telephone calls from that number to be unauthorized access calls to their system.

Schwartz

57. Special Agent Moore's investigation determined that 104 unauthorized telephone calls were made to Source 1's VM computer in March, 1989 from telephone number 614-225-2450 listed to Schwartz in Columbus, Ohio. As part of this investigation a court ordered pen register (DNR) was obtained for the above telephone number on March 31, 1989.

58. Detective Robert Synder's examination of the printouts from the DNR on the Schwartz residence in Columbus, Georgia from April 20, 1989 to May 10, 1989 disclosed that a hacker at that telephone (614-698-2446) was illegally accessing 40 different 800 numbers including the following:

PREFERRED CASES VMS  
COMBUSTION ENGINEERING VMS  
CAP CARE VMS  
KINKO COPIES CORP VMS  
NATIONWIDE MESSAGE CENTER VMB  
MIAMI VOICE VM

The DNR also reflected calls to Augilar's Velayo VMB 800-888-5359 and to the Voudy residence in Georgia (404-594-9892).

59. Special Agent Moore (United States Secret Service - Chicago) has contacted the above referred to companies and learned that they have not authorized anyone named Schwartz at telephone number 614-225-2450 to use their voice mail computer systems and that they regard telephone calls from that number to be unauthorized access to their system.

Evidence of the Crimes Exists

60. Sergeant Abigail Abraham, (Illinois State Police) Det. Bob Snyder (Columbus P.D.) and Tom Schutz (MCI-Chicago), said that in their experience with telephone hackers <sup>in</sup> cases similar to the case here they know that ~~that~~ the hackers use telephones including telephones with speed dialers and memory devices, as well as telephone dialing, signaling devices and electronic tone generating devices to quickly contact other hackers and attack VM computer systems. Sergeant Abraham states that she has reviewed the DNR's in this case and observed the frequency and sequence of numbers being dialed by several of the hackers. Sergeant Abraham states, based upon her experience, several of the hackers are using automatic diallers to quickly scan large groups of numbers to locate access numbers to VM computers and PBX computers and store those numbers. Automatic diallers are then again being used to identify entry codes to enter individual "mail boxes" on the VM computer. Sergeant Abraham further advises that these automatic diallers may exist as part of the telephone equipment at <sup>each</sup> ~~the~~ hackers location or as part of a computer program run by a computer with a modem. Because numerous automatic dialer programs exist for various telephones and computers, it is impossible to specify further which type of dialer program is involved from reviewing the DNR tapes.

61. Detective Snyder, Sergeant Abraham and Tom Schutz further advise that, based upon their experience, computers, computer peripherals and memory storage devices (including disks, cassette tapes, and VCR tapes) are used by telephone hackers as part of their activities. As noted above, computers are frequently used by telephone hackers to automatically dial thousands of telephone numbers to identify VM computers and PBX computers kept by companies and organizations. When a computer hacker "hits" one of these numbers it stores the number for future reference and then continues its scanning operation. The

"hits" are then retrieved by the hacker. If a company's VM computer is identified, hackers then use the computers to dial the possible combinations of the codes on the individual voice mail boxes. Computers are also used by the hackers to telephone numbers of victim companies, unauthorized credit cards and calling cards and computer access codes and passwords, as well as the telephone numbers, names and locator information on other hackers. Computer programs stored either on a computer or on some other storage media may contain specialized hacker programs for breaking computer codes and "blue boxing."

62. Detective Robert Snyder, an experienced telecommunications fraud investigator with the Columbus P.D. states VM computer hackers routinely maintain telephones, telephones with memory devices, speed dialers, voice disguise devices; records of access devices being trafficked in the form of hand written notations or on computerized memory or disk system files and also maintain tape recordings of information and hacker conversation.

63. Information provided by Special Agent Moore confirms that computers are being used by computer hackers in this case. Specifically, during a message left on Proxy VM computer in San Francisco, the Los Angeles hacker at 213-726-4012 stated he was using a computer to break into the VM computer and take control of Proxy's VM computer. During a message the Massachusetts hacker at 617-662-7939 indicated to other hackers on Source 1's VM computer that he was taking access codes obtained from other hackers on Source 1's VM computer and putting them on a computer bulletin board that he was operating on telephone #617-665-7822. (A computer bulletin board is a computer with a modem that carries a series of messages to and from other computer users). Special Agent Moore was also advised by Hank Kluepfel of Bellcore that the PCP numbers trafficked on Source 1's VM computer are access codes to the PC Pursuit computer network and would only be usable to computer operators with modems.

64. Mark S. Yelchak, Senior Technical Investigator, Electronic Operations, Pacific Bell Telephone Company, has advised Special Agent Moore that in his experience telephone hackers currently frequently use and maintain voice and tone distortion equipment near their telephones in an effort to disguise their telephone voice and the dialing tones from telephone security personnel and dialled number recorders (DNR)(pen registers), which may be placed on their telephone lines. Yelchak further advised that this hacker distortion equipment might come in various forms including cassette tape recorders and cassette tapes.

65. Yelchak further advised Special Agent Moore that telephone hackers frequently make and maintain recordings of their voice messages as a form of record of their activities. These recordings are also made with cassette tape recorders and cassette tapes.

66. Yelchak further advised Special Agent Moore that, in an effort to throw off DNR's placed on their telephones by telephone security officers, telephone hackers maintain and use with their telephones equipment which provides a continuous background tone or noise on the telephone line (known by telephone hackers as "pink noise") in an effort to hide and disguise the telephone number that is being called.

67. Gail Thackery, (Arizona's AG's office) has advised Special Agent Moore that on about May 1, 1989 Kyrie called her and said she, Kyrie, had a "black book" of hacker names. During one point where Kyrie was trying to find a hacker's name, Thackery heard papers being rustled as though Kyrie was looking at a source book, log or journal while on the phone. Abrahams and Synder state that other hackers frequently maintain such records and notes of "contacts".

68. Sargeant Abrahm and Detective Synder and Larry Boothby, Physical Security Specialist (United States Secret Service - Chicago) state that special signalling tones can be generated by an electronic tone-generating device known

as a "blue box," or by personal computer and computer software which enables the computer to generate the tone signal through a communications device (a modem or acoustic coupler) connecting the computer to the telephone line. In their past investigations, Sargeant Abraham and Detective Snyder have frequently found that persons stealing communications services have possessed a personal computer and the necessary software which would allow them to manipulate communications networks by means of the special signalling tone.

69. Detective Snyder states that in his experience hackers sometimes maintain "degaussing devices" at or near their equipment, to erase electronic storage in the event of a search. The purpose of degaussing equipment is to rapidly erase magnetic media.

70. Sargeant Abraham, Detective Snyder and Schutz (MCI-Chicago) also state that, based upon their experience, the hackers in this case will maintain written notes, records, journal and tape recordings (cassette and VCR tapes) relating to their hacking activities and contacts. They will also maintain notes and records of credit card transactions and purchases on the credit cards.

Need For Removing Telephone and Computer Systems  
From Premises and Taking Software

71. Special Agent Moore interviewed Special Agent Steve Purdy of the U.S. Secret Service, Washington, D.C. Purdy informed Moore that in connection with his employment, he uses computer systems, and conducts computer related investigations for the United States Secret Service Fraud Unit in Washington, D.C. In the last two years Special Agent Purdy has supervised or participated in several executions of search warrants for computer stored records and evidence. Special Agent Purdy informed Special Agent Moore that because computer stored data is vulnerable to destruction through error, magnetic fields, electrical outages and other causes, most computer users keep "backup copies" of their data and programs. These copies can be found on floppy diskettes, tape cassettes and other storage media. Special Agent Purdy stated that even if data is erased or deleted

from the system itself, it might be found on the backup copies.

72. Special Agent Purdy stated that when records are stored on floppy disks or on a hard disk, even when they appear to have been erased or deleted, they may still be retrievable. Special Agent Purdy is familiar with the methods of restoring "lost" data commonly employed by computer users and has used those methods himself and has also used the assistance of a computer expert in several cases in order to obtain the contents of computer stored evidence.

73. Special Agent Purdy stated that conducting a search of a computer system, documenting the search and making evidentiary copies is a lengthy process. It is necessary to determine that no security devices are in place which could cause the destruction of evidence during the search. In some cases it is impossible even to conduct the search without expert assistance. Since computer evidence is extremely vulnerable to tampering or destruction, removal of the system from the premises will assist in retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would be extremely difficult to secure the system on the premises during the search, especially when it is connected by modem to communications lines. Destruction or alteration could be performed from a location remote from the premises during the search.

74. Special Agent Purdy also stated that the accompanying software must also be seized since it would be impossible without examination to determine that it is standard, commercially available software. It is necessary to have the software used to create data files and records in order to read the files and records.

75. Special Agent Purdy stated that in his experience there are other memory storage devices involving similar problems, such as telephones with programmable memories, and "credit card computers" used to store calendars, telephone numbers and addresses, and even financial records. He stated that in his experience each



of these types of technology could or would be used by vM hackers during the course of their activities.

#### Locations To Be Searched

##### Doucett

76. Special Agent Moore has been advised by Roland Kwasney of Illinois Bell Telephone Company, Security Division, that their records reflect that telephone line 312-262-7217 is physically located in Apartment 204 in the apartment building at 6748-6750 North Ashland Avenue, Chicago, Illinois.

77. Your affiant has been to the building described as 6748-6750 North Ashland Avenue in Chicago which contains telephone 312-262-7217. That location is truly and accurately reflected in the attached photographs and is further described as a multi-story apartment building with the numbers 6748 on the front door. Inside the front door 6748 shares a common lobby with 6750 North Ashland. (Attachment 1).

##### Aguilar

78. Your affiant has been advised by agents of the U.S. Secret Service in Los Angeles that the location containing the 212-726-4012 telephone number is described as follows: 6302 Hereford Drive is located on the southeast corner of Hereford Drive and Saybrook Street in Los Angeles, California, corner lot. It is a light beige colored one-story house with white wood trim and a brown colored shingle roof. The outside perimeter of the yard is surrounded by a white picket fence approximately 2-3 feet tall. The garage is unattached and is located in the rear of the residence off of Saybrook Street. It is in the far southwest corner of the yard. The front door is a dark colored metal type security screen door located in the center of the front of the house. An approximately 12 inch x 4 inch piece of what appeared to be wood is suspended from the ceiling outside the front door, white in color, with the numbers "6302" on it, also white in color.

"6302" is also painted on the curb outside the front of the house on Hereford Street, numbers black with a white painted background. A fire hydrant is located by the front yard gate off of Hereford, outside of the gate, while inside the gate, approximately 10 feet east of the gate a white mailbox stands. Approximately 12 foot tall bushes surround the front and west side of the house, except the eastern front of the house which has approximately 3 foot tall bushes. All of this foliage is on the outside perimeter of the yard behind the white picket fence. There is a considerable amount of shrubery all around the residence. A white street lamp and pole is located on the west side of the house by the Saybrook Street curb near the corner of Saybrook and Hereford Drive. ~~(See attached photographs)~~

#### Colley

79. Your affiant has been advised by agents of the U.S. Secret Service in Detroit that the location containing the 313-247-9252 telephone number is described as follows: 14338 Pernell Drive, Sterling Heights, Michigan is further described as a single family, one story, brick exterior, brown in color, brown roof, beige trim above brick with dark brown wooden trim strips over the beige paint, on the south side of Pernell between Schoenher and Saal Drive in Sterling Heights, Michigan. The address is marked on a trim strip above the garage door on the front on the house. ~~(See attached photographs)~~

#### McMahon

80. Your affiant has been advised by agents of the U.S. Secret Service in Boston that the location containing the 617-662-7939 telephone number is described as follows: the McMahon residence at 141 Waverly Avenue in Melrose, Massachusetts is further described as a yellow single family residence with a hip roof, brown shutters and trim on the house and a screened in front porch in front of the residence. The numbers "141" are located on the front door of the residence which faces Waverly Street and is approximately 15 feet from the front sidewalk. ~~(See attached photographs)~~

#### Voudy

81. Agents of the U.S. Secret Service in Atlanta, Georgia have observed

and describe the location containing the 404-642-1987 telephone number as follows: 1722 Thorrs Rook, Marietta, Georgia is a two-story contemporary, single family dwelling with brown wood siding located on a slightly elevated wooded lot with "1722" on the mail box next to the driveway leading to the attached garage of the residence. ~~(See attached photographs.)~~

Schwartz

82. Your affiant has been advised by agents of the U.S. Secret Service in Columbus that the location containing the 614-225-2450 telephone number is described as follows: 5893 Effingham Road, Columbus, Ohio is further described as a split-level, Tudor design single family residence which is one-half brick and one-half stucco, which is being in color with brown trim and brown shutters. A two-car garage with a brown door is built into the house and the drive-way running from the street to the garage is lined with railroad ties and has a red basketball post with no backboard on the edge. The numbers "5893" are on the mail box post near the road near the driveway. ~~(See attached photographs.)~~

Evidence to be Seized

83. Based upon the above described facts, details and circumstances and information provided by Secret Service personnel and other law enforcement officers familiar with computer fraud and telecommunication fraud investigations, your affiant believes that the following list of items are the types of computer hardware and software and telephone equipment, some or all of which would be used by "hackers" to obtain and/or use unauthorized security codes, including the following:

1. telephones including memory devices and associated peripheral equipment, including automatic diallers, speed diallers, programmable telephone dialling or signalling devices, electronic tone generating devices;
2. computers, central processing units, external and internal drives and external and internal storage equipment or media, terminals or video

display units, together with peripheral equipment such as keyboards, printers, modems or acoustic couplers, automatic diallers, speed diallers, programmable telephone dialling or signalling devices, electronic tone-generating devices;

3. computer or data processing software, or data including, but not limited to: hard disks, floppy disks, cassette tapes, video cassette tapes, magnetic tapes, integral RAM or ROM units, and any other permanent or transient storage device(s);
4. the following records and documents, whether contained on paper in handwritten, typed, photocopied or printed form, or stored on computer printouts, magnetic tape, cassettes, disks, diskettes, photooptical devices, or any other medium: telephone and communications activity and service billing records, computer electronic and voice mail system information, access numbers, passwords, personal identification numbers (PINS), telephone and address directories, logs, notes, memoranda and correspondence relating to theft of telephone and communications services, or to unauthorized access into computer, electronic and voice mail systems;
5. any computing or data processing literature, including, but not limited to: printed copy, instruction books, notes, papers, or listed computer programs, in whole or in part;
6. Indicia of occupancy, including, but not limited to: bills, letters, invoices, personal effects, rental agreements tending to show ownership, occupancy, or control of the premises, or the above-described items one through three;
7. confirmation numbers, purchase numbers, and purchase information reflecting the use of a credit card to obtain property, goods or service;

and

8. degaussing equipment located at the search location.

84. Based upon all the foregoing, your affiant believes that probable cause exists for the issuance of a search warrant for the search, seizure, review and maintenance of the above described located at Apartment 204 in the multi-story apartment building located at 6748-6750 North Ashland Street in Chicago, Illinois and any other area physically connected to the telephone line (312) 262-7217. (See Attachment 1, photographs of the exterior of 6748-6750 North Ashland, Chicago, Illinois.)

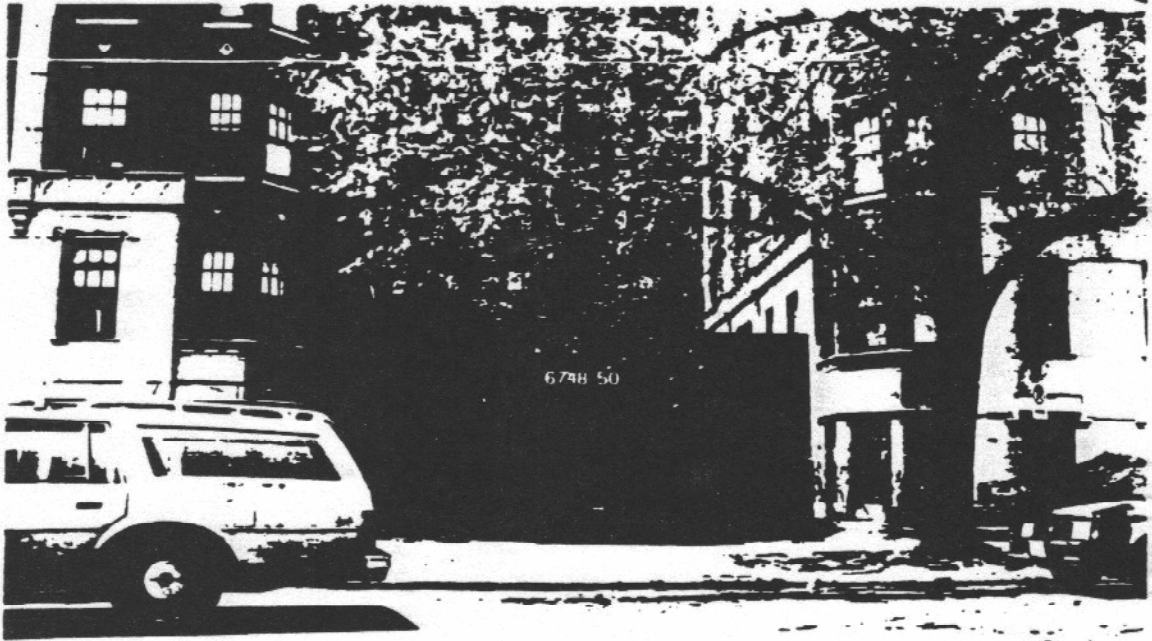
\_\_\_\_\_  
Affiant

Subscribed and sworn to me this \_\_\_\_\_ day of May, 1989.

\_\_\_\_\_  
United States Magistrate

WJC:jan(A/1)

Attachment 1



## Attachment 2

The following property is concealed:

1. Any and all telephones including memory devices and associated peripheral equipment, including automatic diallers, speed diallers, programmable telephone dialling or signalling devices, electronic tone generating devices.

2. Computers, central processing units, external and internal drives and external and internal storage equipment or media, terminals or video display units, together with peripheral equipment such as keyboards, printers, modems or acoustic couplers, automatic diallers, speed diallers, programmable telephone dialling or signalling devices, electronic tone-generating devices;

3. Any and all computing or data processing software, or data including, but not limited to: hard disks, floppy disks, cassette tapes, video cassette tapes, magnetic tapes, integral RAM or ROM units, and any other permanent or transient storage device(s).

4. The following records and documents, whether contained on paper in handwritten, typed, photocopied or printed form, or stored on computer printouts, magnetic tape, cassettes, disks, diskettes, photooptical devices, or any other medium: telephone and communications activity and service billing records, computer electronic and voice mail system information, access numbers, passwords, personal identification numbers (PINS), telephone and address directories, logs, notes, memoranda and correspondence relating to theft of telephone and communications services, or to unauthorized access into computer, electronic and voice mail systems;

5. Any computing or data processing literature, including, but not limited to: printed copy, instruction books, notes, papers, or listed computer programs, in whole or in part;

6. Indicia of occupancy, including, but not limited to: bills, letters, invoices, personal effects, rental agreements tending to show ownership, occupancy, or control of the premises, or the above-described items one through three.

7. Any confirmation numbers, purchase numbers, and purchase information reflecting the use of a credit card to obtain property, goods or services.

8. Neutralize and seize degaussing equipment located at the search location.

This affidavit recognizes that some of the above described property is data that will be contained on cassette tapes, video tapes and in electronic and machine readable media which is not readable by your affiant in its present state. By this affidavit your affiant requests authorization for himself and other searching agents to seize, listen to, read, review and maintain the above described property and to convert it to human readable form as necessary. Your affiant is advised that data stored in computers and telephone memory machines may be lost if it is disconnected from an electrical power source. Your affiant by this affidavit therefore additionally requests authorization to make human readable copies or recordings of this data at the search location in order to preserve and protect the information, and to thereafter seize, read, listen to and maintain the described property.