THE WHITE HOUSE

WASHINGTON

October 14, 1983

MEMORANDUM FOR FRED F. FIELDING

FROM: JOHN G. ROBERTS

SUBJECT: Testimony of Floyd Clarke on Computer Crime - October 17, 1983

We have been provided with a copy of the testimony that FBI Deputy Assistant Director Floyd Clarke proposes to deliver on Monday before the House Subcommittee on Transportation, Aviation and Materials. The testimony concerns computer related crime. Clarke makes clear that the FBI does not have accurate statistics on computer related crime, since the Bureau does not break down crimes according to whether computers were involved. He reviews several recent FBI investigations into computer piracy, and expresses general support for H.R. 3970 and S. 1733, bills designed to improve federal computer crime legislation. The proposed testimony concludes by noting that the computer and communications systems of the FBI would be enhanced by greater security systems. In particular, Clarke urges voice protection measures for the Bureau's radio system. The Administration has asked Congress for funds for this purpose in the past.

I have reviewed the proposed testimony, and have no objections to it.

Attachment

THE WHITE HOUSE

WASHINGTON

October 15, 1983

MEMORANDUM FOR BRANDEN BLUM
LEGISLATIVE ATTORNEY
OFFICE OF MANAGEMENT AND BUDGET

FROM: FRED F. FIELDING Orig. signed by FFF
COUNSEL TO THE PRESIDENT

SUBJECT: Testimony of Floyd Clarke on Computer Crime - October 17, 1983

Counsel's Office has reviewed the above-referenced testimony, and finds no objection to it from a legal perspective.

FFF:JGR:aea 10/14/83

cc: FFFielding
JGRoberts
Subj
Chron

THE WHITE HOUSE

WASHINGTON

October 15, 1983

MEMORANDUM FOR BRANDEN BLUM
LEGISLATIVE ATTORNEY
OFFICE OF MANAGEMENT AND BUDGET

FROM: FRED F. FIELDING
COUNSEL TO THE PRESIDENT

SUBJECT: Testimony of Floyd Clarke on Computer Crime - October 17, 1983

Counsel's Office has reviewed the above-referenced testimony, and finds no objection to it from a legal perspective.

FFF:JGR:aea 10/14/83

cc: FFFielding
JGRoberts
Subj
Chron

ID # _____ CU

WHITE HOUSE
CORRESPONDENCE TRACKING WORKSHEET

☐ O - OUTGOING
☐ H - INTERNAL
☐ I - INCOMING
Date Correspondence Received (YY/MM/DD) / /

JR

Name of Correspondent: Branden Blum

☐ **MI Mail Report** **User Codes: (A)** _____ **(B)** _____ **(C)** _____

Subject: Testimony of Floyd Clarke on Transportation, Aviation and Materials - October 17, 1983

ROUTE TO: / **ACTION** / **DISPOSITION**

Office/Agency (Staff Name)	Action Code	Tracking Date YY/MM/DD	Type of Response	Code	Completion Date YY/MM/DD
W Holland	ORIGINATOR	83/10/14			/ /
	Referral Note:				
CWAT18	D	83/10/14		S	83/10/15
	Referral Note:				
		/ /			/ /
	Referral Note:				
		/ /			/ /
	Referral Note:				
		/ /			/ /
	Referral Note:				

ACTION CODES:
A - Appropriate Action
C - Comment/Recommendation
D - Draft Response
F - Furnish Fact Sheet to be used as Enclosure
I - Info Copy Only/No Action Necessary
R - Direct Reply w/Copy
S - For Signature
X - Interim Reply

DISPOSITION CODES:
A - Answered
B - Non-Special Referral
C - Completed
S - Suspended

FOR OUTGOING CORRESPONDENCE:
Type of Response = Initials of Signer
Code = "A"
Completion Date = Date of Outgoing

Comments: _____

Keep this worksheet attached to the original incoming letter.
Send all routing updates to Central Reference (Room 75, OEOB).
Always return completed correspondence record to Central Files.
Refer questions about the correspondence tracking system to Central Reference, ext. 2590.

5/81

DRAFT

TESTIMONY OF

DEPUTY ASSISTANT DIRECTOR

FLOYD I. CLARKE

CRIMINAL INVESTIGATIVE DIVISION

FEDERAL BUREAU OF INVESTIGATION

WASHINGTON, D. C.

BEFORE THE

HOUSE SUBCOMMITTEE

ON

TRANSPORTATION, AVIATION, AND

MATERIALS

OCTOBER 17, 1983

Thank you Mr. Chairman for providing me an opportunity to present the FBI's views on the subject of telecommunications, security and privacy, and to respond to your specific areas of concern.

Prior to responding to your specific questions, I would like to point out three things that we in the FBI believe are key to understanding the FBI's perspective on computer related crimes.

The first of these issues is that a computer is an instrumentality of some other form of traditional crime, for instance theft or larceny. It is much like a gun, a knife, or a forger's pen.

The second issue is of a more academic nature, but nevertheless important in that there does not exist, at this time, one generally recognized and accepted definition as to what computer related crime is. Therefore, we do not have an objective standard to measure the trends of computer related crime.

Lastly, in view of the FBI's current structure of management by program, rather than by case, there is no method in place now to observe the statistical dimensions of computer related crime.

With that in mind, I would like to discuss the nature, extent, and dimensions of crimes involving computers and communications from the FBI's perspective.

As you are aware, there is no one agency at this time that has jurisdiction for computer related crimes and very probably there cannot be because of the wide application of computers. The FBI's jurisdiction in computer related crimes is derived from jurisdiction previously assigned to the FBI by Congress or the Attorney General of the United States in more traditional areas. Generally speaking, the statutes most frequently used by the Department of Justice and the FBI to prosecute and investigate computer related crimes are Fraud by Wire, Interstate Transportation of Stolen Property, Bank Fraud and Embezzlement, Destruction of Government Property, and Theft of Government Property. However, computer related crimes transcend

all the crime categories and jurisdictions, local, state and Federal, again making it difficult to measure trends in this type of crime.

Another problem that has been encountered is a reluctancy on the part of some businesses, especially those in the financial community, to report losses attributable to computer related crimes in an attempt to avoid developing an image of fiscal insecurity. Therefore, in the absense of a generally accepted definition of computer related crime, coupled with the lack of a central repository for the statutes on computer related crimes, it would appear the current position in response to your question as to the extent of computer related crime is that no one knows for sure.

Since the early 1970's, the FBI has been involved in computer related crime investigations, and with our limited scope to track computer related crime we have noted no dramatic increase in this type of crime. Logic would indicate that with the ever increasing number of computers in use today, there ought to be a corresponding increase in computer related crimes; however, we have no credible documentation to support this sort of conclusion.

As to the dimension of computer related crimes, there is a large potential for extremely large losses. Most financial institutions, our government and governments of other countries, utilize computers to facilitate their operations. This creates a potential for abuse by persons who have the necessary knowledge, time and access to the correct hardware or software. In a very short period of time, programs, high technology information, proprietary information or classified information can be taken from a computer without leaving much evidence of the crime. This is to say nothing of wire transfers of large amounts of money between financial institutions.

In response to your request for illustrations of computer related crime that the FBI has been involved in, I would like to bring to your attention some specific instances of these type crimes.

In 1979, the New York Division of the FBI identified a computer information service company (which is a company that enters, edits, stores, and retrieves information in a text format) that was, without authorization, accessing and modifying records of a similar computer information service in the State of California. The second computer service was the primary competitor to the first and the actions of the first computer service caused an estimated loss of $7.5 million.

In 1980, the New York Division again identified a group of children of middle school age who accessed without authorization, over 20 computers from the computer located at their school. The unauthorized accesses by this group in both the United States and Canada not only caused the loss of computer time and disrupted computer services, but caused the destruction of inventory and billing figures of a Canadian firm, which necessitated substantial efforts by that firm to duplicate.

In late 1982, our Washington Field Office identified a former employee of the Federal Reserve Bank who was then employed privately as a financial analyst, who attempted to continue to access information in the Federal Reserve Bank's money one file without authorization. Any information he might have obtained from this file would have been useful in the analysis of his client's holdings.

Early in 1983, our office in Alexandria, Virginia, identified an individual who without authorization accessed computerized consumer credit information to obtain credit account information on over 80 people. Thereafter he used this information to charge goods including additional computer equipment to the major credit cards of the people whose credit information he had accessed.

More recently, a great deal of media coverage has been afforded our efforts in an investigation of a computer related matter in the Mid-West. That matter is currently pending prosecution.

These examples are certainly not all inclusive of our efforts in computer related crimes, but they give a broad view of the types of computer related crimes that are presented to the FBI for investigation. We have so far been able to identify and locate the person(s) committing each of the beforementioned crimes. We hope to continue to due so.

We have also had successful prosecutions in all but two of these matters. Prosecution was mitigated in one instance by the age of the subjects, and the other matter is pending prosecution now.

We in the FBI have not had, to date, any significant problems in prosecution of computer related crime under already existing statutes over which we have jurisdiction, such as the Fraud by Wire Statute.

There are currently two bills pending before Congress which would provide Federal computer crime legislation. These bills are HR 3970, introduced by Congressman Bill Nelson of Florida, and S 1733, introduced by Senator Paul Tribble of Virginia. We support both bills in principle.

There are currently some 21 states that have specific computer legislation to address computer related crime on a local and state level.

Our experience indicates that certain legal issues involving computer related crime could be clarified, particularly the definition of property in the sense of a computer program having its own clearly defined inherent value and the issue of trespass. The most frequently heard defense for simple unauthorized access into someone else's computer is that the individual making the access has no criminal intent, meant no harm, there was no security system and therefore there is no trespass. However, it is fairly commonly held that if an individual without authorization enters the unlocked house of another and rummages through that person's closets with no intent to steal or to do harm that person could still be guilty of trespassing. It is important that a legal clarification be made in this regard.

In regard to preventive measures necessary to deal with computer related crime it appears from our experience that this is more of a human problem than a technological one. In most instances where we have been involved in an investigation of computer related crime the crime was perpetrated by someone who had access to the computer and authorization to use it. The crime was facilitated by the access and in most cases the authorization was exceeded or misused.

In conclusion, I would like to address the need of law enforcement agencies for computer and communications security and privacy in their own operations. It is a well documented fact that government law enforcement agency radio communications are monitored

by non-law enforcement elements, ranging from the hobbyist, who gains a vicarious thrill from being "in" on law enforcement operations, to the entrepreneur, who listens for profit; the news media or the person who markets lists of government frequencies exhibiting interesting activity, to the criminal who listens to evade law enforcement operations as well as the foreign intelligence operative. These elements monitor our radio circuits to gain information on our operations, through intercept and analysis of our radio traffic; to disrupt operations by learning of our movements in advance and evading or countering them; to identify and associate agents with ongoing operations. In short, we pay a severe penalty due to the vulnerability of our clear text voice radio system used to control our operations. We pay this penalty in terms of personnel overhead. Up to 20% of a surveillant's time may be spent to accomodate the verbal codes, additional surveillance vehicles, and other burdens imposed to protect operations. There are compromised cases, wherein hundreds of hours of effort may be wasted because the subject learned of our operations by monitoring our circuits and successfully evaded apprehension or, forewarned, was able to destroy vital evidence, thus jeopardizing prosecution. There is a hazard to Agents, Agent identity, location or cover, and if compromized, it could place him in a highly dangerous position. Subjects have used intercepted radio transmissions to identify and endanger the life of operatives.

To counter the threat, voice protection measures must be applied to our radio system. In our counterintelligence operations, national defense is at stake and full speech "security" is required. In conducting our law enforcement operation; however, a significant

deficiency exists in countering the known threat. In this area, speech security is not always warranted, but there is a distinct and pressing need for voice "privacy" on our radio system nationwide.

This concludes my prepared remarks Mr. Chairman. I will be happy to address any questions you may have.

THE WHITE HOUSE

WASHINGTON

November 9, 1983

MEMORANDUM FOR FRED F. FIELDING

FROM: JOHN G. ROBERTS JGR

SUBJECT: Statement of John Keeney Regarding Credit Card and Computer Fraud H.R. 3570 and H.R. 3181 on November 10, 1983

Deputy Assistant Attorney General John Keeney proposes to deliver the attached testimony before the House Judiciary Subcommittee on Crime on November 10. Keeney's testimony discusses two bills, H.R. 3570 and H.R. 3181, which provide penalties for credit and debit card counterfeiting and other related fraud. H.R. 3570 also provides penalties for anyone who "uses a computer with intent to execute a scheme to defraud."

The testimony expresses strong support for the portions of both bills dealing with crimes involving credit and debit cards. Like other testimony delivered on behalf of the Administration on this subject, this statement suggests various amendments to the bill to correct problems caused by judicial decisions, such as the fact that illegal use of a credit card number, as opposed to the card itself, is not covered. The testimony also suggests that the provisions dealing with computer fraud be severed from the legislation, so that Justice and other agencies have more time to study possible solutions to the problem. I have reviewed the testimony, and find no objections to it.

Attachment

THE WHITE HOUSE

WASHINGTON

November 9, 1983

MEMORANDUM FOR GREGORY JONES
LEGISLATIVE ATTORNEY
OFFICE OF MANAGEMENT AND BUDGET

FROM: FRED F. FIELDING Orig. signed by FFF
COUNSEL TO THE PRESIDENT

SUBJECT: Statement of John Keeney Regarding Credit Card and Computer Fraud H.R. 3570 and H.R. 3181 on November 10, 1983

Counsel's Office has reviewed the above-referenced testimony, and finds no objection to it from a legal perspective.

FFF:JGR:aea 11/9/83
cc: FFFielding/JGRoberts/Subj/Chron

THE WHITE HOUSE

WASHINGTON

November 9, 1983

MEMORANDUM FOR GREGORY JONES
LEGISLATIVE ATTORNEY
OFFICE OF MANAGEMENT AND BUDGET

FROM: FRED F. FIELDING
COUNSEL TO THE PRESIDENT

SUBJECT: Statement of John Keeney Regarding Credit Card and Computer Fraud H.R. 3570 and H.R. 3181 on November 10, 1983

Counsel's Office has reviewed the above-referenced testimony, and finds no objection to it from a legal perspective.

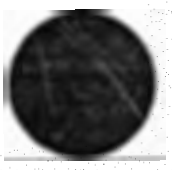
FFF:JGR:aea 11/9/83
cc: FFFielding/JGRoberts/Subj/Chron

ID # CU

WHITE HOUSE
CORRESPONDENCE TRACKING WORKSHEET

John

☐ O - OUTGOING
☐ H - INTERNAL
☐ I - INCOMING
Date Correspondence Received (YY/MM/DD) / /



Name of Correspondent: Greg Jones

☐ **MI Mail Report** **User Codes:** (A) _____ (B) _____ (C) _____

Subject: Statement of John Keeney re: Credit Card and Computer Fraud H.R. 3570 and H.R. 3181 on November 10, 1983

ROUTE TO:

Office/Agency (Staff Name)	Action Code	Tracking Date YY/MM/DD	Type of Response	Code	Completion Date YY/MM/DD
CWHOU	ORIGINATOR	83/11/04			/ /
	Referral Note:				
CWAT18	D	83/11/04		S	83/11/09
	Referral Note:				
		/ /			/ /
	Referral Note:				
		/ /			/ /
	Referral Note:				
		/ /			/ /
	Referral Note:				

ACTION CODES:
A - Appropriate Action
C - Comment/Recommendation
D - Draft Response
F - Furnish Fact Sheet to be used as Enclosure
I - Info Copy Only/No Action Necessary
R - Direct Reply w/Copy
S - For Signature
X - Interim Reply

DISPOSITION CODES:
A - Answered
B - Non-Special Referral
C - Completed
S - Suspended

FOR OUTGOING CORRESPONDENCE:
Type of Response = Initials of Signer
Code = "A"
Completion Date = Date of Outgoing

Comments: _____

Keep this worksheet attached to the original incoming letter.
Send all routing updates to Central Reference (Room 75, OEOB).
Always return completed correspondence record to Central Files.
Refer questions about the correspondence tracking system to Central Reference, ext. 2590.

5/81

DRAFT

STATEMENT

OF

JOHN C. KEENEY
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE

THE

SUBCOMMITTEE ON CRIME
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

CONCERNING

CREDIT CARD AND COMPUTER FRAUD
H.R. 3570 and H.R. 3181

ON

NOVEMBER 10, 1983

Mr. Chairman and Members of the Subcommittee, I am pleased to be here today to present the views of the Department of Justice on two bills, H.R. 3570, the "Counterfeit Access Device and Computer Fraud Act of 1983," and H.R.3181, the "Credit Card Counterfeiting and Fraud Act of 1983." The Department strongly supports in concept the portions of the two bills that deal with various crimes involving credit and debit cards although we will suggest various drafting changes along the way.

We can also understand the desire to provide a federal sanction against computer fraud as is done in H.R. 3570, since, to a certain extent, computer fraud and credit and debit card offense are related. Nevertheless, at this juncture, we strongly urge that the two issues be severed and that legislation be processed relating only to credit and debit card crimes. The reason is that, quite frankly, the Department of Justice has not reached a position on the desirability and scope of specific legislation in this area, nor is it clear that there exists sufficient information about the extent and nature of computer crime to formulate such views, although from what we have been able to determine preliminarily, federal legislation may indeed be necessary. In response to a request from the Attorney General, an intradepartmental task force is now actively studying this issue and we hope to have a set of recommendations for the Congress in the relatively near future. That consideration of specific computer crime legislation may be premature at this time is underscored by the action taken by the House in its passage on October 24th of H.R. 3075, "The Small Business Computer Crime

Prevention Act." As you probably know, Mr. Chairman, that act does not create any new offenses but requires the Small Business Administration to establish a task force to study several aspects of computer crime.

Consequently, I will today confine my remarks to credit and debit card crimes, an area which has received a good deal of attention in the Congress, and on which there is a general consensus that new federal statutes are in order. I might also add, Mr. Chairman, that we think the need for legislation in the card area is such that we hope it will not be delayed pending either the Justice Department's or the Small Business Administration's study of the computer crime problem.

Turning then to the question of credit and debit card offenses, I think it would be useful first to describe for the Subcommittee the recent efforts of the Department in attempting to deal with the problems of credit card and debit card counterfeiting and fraud. For more than a year, officials of the Criminal Division and of the Federal Bureau of Investigation have been meeting with bank and bank card industry representatives concerning problems that have developed with the enforcement of the criminal provisions of the Truth in Lending Act, 15 U.S.C. 1644, which covers credit cards, and with the similar criminal provisions in the Electronic Fund Transfers (EFT) Act, 15 U.S.C. 1693n, which covers debit cards. These contacts with the industry have made us very much aware of the dramatic increase in the counterfeiting and the fraudulent use of credit cards. We

are also familiar with the major increase in EFT activity through a preliminary study done by the Department's Bureau of Justice Statistics in June of 1982, and our conversations with industry representatives. This increase creates the distinct possibility of a sharp upswing in crimes involving EFT systems and their accompanying debit cards.

Our concern in this area, however, is not with the high volume, low dollar losses of present or future credit or debit card transactions. The average credit or debit card fraud loss is so small that the crime can generally be prosecuted on a local level wnere personnel resources are much greater than those available to the federal government.[1]

Rather, our concerns have focused primarily on four issues. They are: (1) the lack of current statutory coverage over the burgeoning problem of counterfeiting credit and debit cards; (2) the need to clarify 15 U.S.C. 1644 so as to reach the misuse of another person's card number, in addition to the plastic card

---

[1] To do our part in ensuring that these matters are, in fact, handled by state or local prosecutors, officials in the Department of Justice have worked closely with the state Attorneys General and local District Attorneys through our Executive Working Group of Federal, State and Local Prosecutors on a national level, and the Law Enforcement Coordinating Committees on a state and local level. Our contact with our state and local counterparts has convinced us that while some improvements in existing federal laws are needed, there is no need for the massive federal involvement in areas of traditional local concern, such as minor fraud cases, that would result if virtually every credit card crime were made a federal offense, the approach of some early draft bills prepared by the banking and credit card industry.

itself;[2] (3) the gap in the present credit card fraud provisions in the Truth in Lending Act which has been construed not to reach transactions in which a credit card is originally obtained without fraudulent intent from a card issuer but subsequently transferred to another person with the knowledge that it will be fraudulently used;[3] and (4) the difficulties arising from the current monetary jurisdictional limitation in the Acts which, as presently written, allow a person to use unlawfully one card, accumulate just under $1,000 worth of purchases, discard it, and use another card to do the same thing without committing a federal violation.

---

2 The Ninth circuit, in United States v. Callihan, 666 F.2d 422 (1982), held that only misuse of a card, not the card number, is prohibited by the statute. By contrast, the Fourth Circuit has held that the fraudulent use of a credit card number is covered by 15 U.S.C. 1644(a). See United States v. Bice-Bey, 701 F.2d 1086, 1091-1092 1983).

3 15 U.S.C. 1644(a) criminalizes the actions of one who "knowingly in a transaction affecting interstate or foreign commerce, uses or attempts or conspires to use any counterfeit, fictitious, altered, forged, lost, stolen or fraudulently obtained credit card to obtain money, goods, services, or anything else of value which within any one-year period has a value aggregating $1,000 of more." (Emphasis added) 15 U.S.C. 1693n (b)(1) tracks this language for debit cards. In United States v. Kasper, 483 F. Supp. 1208 (E.D Pa., 1980), the court held that 15 U.S.C. 1644(a) did not cover the situation where credit cards were obtained by the original cardholders without the intent to defraud the issuing companies, subsequently sold or given to the defendants with the knowledge of the original cardholders that the defendants would use them to make charges without paying for them, and the cards then reported as lost or stolen.

In our view, both H.R. 3181 and H.R. 3570 effectively cover the counterfeiting of credit and debit cards, and also contain important provisions prohibiting the sale, transfer, or possession of equipment used in making phony cards. Thus, both bills take a substantial step in dealing with card counterfeiting, the most important offense in this area.

However, these bills only partially overcome the problems created by the Kasper case concerning the meaning of the phrase "fraudulently obtained" and the problems created by the Callihan case concerning the existing statutes' lack of coverage of card numbers. We note parenthetically that the two bills do not deal with the "accumulation issue", the gap in the present law whereby a person can purchase just under $1,000 worth of goods with one stolen or lost card, then purchase just under $1,000 worth of goods with a second such card, and continue this activity indefinitely without violating the statute. We do not mean this as criticism of the scope of H.R. 3181 and 3570, for as you know the issue of the fraudulent use of a card number and the accumulation issue are dealt with in H.R. 3622, a bill reported by the Banking Committee on October 6th and presently awaiting floor action.

Inasmuch as H.R. 3622 does not, however, deal with the issue of the judicial construction of the phrase "fraudulently obtained" in the Kasper case, I would like to explain briefly how the two bills pending here, H.R. 3181 and H.R. 3570, in our view require some modification in order effectively to overcome the

holding in that case. Both bills add a new section 1029 to title 18. In H.R. 3181, the section would proscribe the knowing production, sale, or transfer of a "fraudulent payment device," while in H.R. 3570, the section would prohibit such production, sale, or transfer of a "fraudulent access device." The two terms are defined virtually identically.[4] However, the actual use of the credit card to obtain goods by the person who purchases the card from, or is given it by, the original holder -- one of the offenses charged in Kasper -- is not covered in either bill. Moreover, neither bill would directly cover a person who obtained a card for no consideration[5] although it would cover a person who bought the card from its original owner and the original cardholder who sold it or gave it away.

These problems may be resolved by minor amendments to H.R. 3181 and H.R. 3570, and we would be pleased to work with the Subcommittee and its staff to accomplish this goal. We also

---

[4] In H.R. 3181, the term "fraudulent payment device" is defined as "(A) any payment device or a representation, depiction, facsimile, aspect or component of a payment device that is counterfeit, fictitious, altered, forged, lost, stolen, incomplete, fraudulently obtained or obtained as part of a scheme to defraud; or (B) any invoice, voucher, sales draft, or other reflection or manifestation of such a device."

In H.R. 3570, the term "fraudulent access device" is defined as "any access device or a representation, depiction, facsimile, or component of an access device that is counterfeit, fictitious, altered, forged, lost, stolen, incomplete, fraudulently obtained or obtained as part of a scheme to defraud."

[5] The person might be chargeable under 18 U.S.C. 2 as an aider and abettor of the transferror, but this seems a peculiarly oblique method of punishing the conduct.

suggest that the Subcommittee may wish to review the question of whether to address the issue of clarifying the coverage of the misuse of card numbers, in view of the adequate resolution of this issue in the Banking Committee bill.

A final suggestion, Mr. Chairman, is that while we believe it is both important and appropriate to cover card counterfeiting in title 18, we would prefer that the description of the device counterfeited or altered be set out by cross-reference to the existing definitional sections of the Truth in Lending and EFT Acts (15 U.S.C. 1602(k) and 15 U.S.C. 1693n(c)). This approach avoids the problem of introducing into the law multiple and confusing definitions of credit and debit devices in two different titles of the United States Code.

In sum, Mr. Chairman, we support the thrust of these bills to the extent that they proscribe debit and credit card counterfeiting in title 18, but suggest that the objects counterfeited be defined by reference to the definitional sections of the Truth in Lending and EFT Acts. The three other problems in the enforcement of those Acts which I have discussed can perhaps best be overcome by amendments to those Acts, as is proposed with respect to two of the three issues in the pending Banking Committee bill. If, however, the Subcommittee decides to attempt to deal in its legislation with the problem caused by the Kasper case whereby a card is not considered "fraudulently obtained"

unless it was so obtained by the original holder, we think that an amendment is needed to cover the actual use of such a card to obtain goods or services.

Mr. Chairman, that concludes my prepared testimony, and I would be pleased to try to answer any questions the Subcommittee may have.

THE WHITE HOUSE

WASHINGTON

November 17, 1983

MEMORANDUM FOR FRED F. FIELDING

FROM: JOHN G. ROBERTS JGR

SUBJECT: Statement of John C. Keeney
Re: Computer Crime -- H.R. 1092
on November 18, 1983

We have been provided with a copy of the above-referenced testimony, which Deputy Assistant Attorney General Keeney proposes to deliver before the House Judiciary Subcommittee on Civil and Constitutional Rights on November 18. The testimony notes that the Department is still reviewing the question of computer fraud, and that it hopes to submit proposals in the near future. Accordingly, Keeney takes no position on proposals currently pending before the Subcommittee. He does note that computer fraud fits uncomfortably into existing criminal provisions, with gaps caused by requirements such as the need for transmissions to cross state lines to be covered by federal law or the need to consider theft of information the theft of a tangible asset with fixed value.

Keeney defers to Commerce on a proposal to fund a grant program to develop new methods of protecting computers, and to Treasury on a proposal to give tax credits to those who purchase computers. He does object to a plan to create an interagency advisory committee on the subject as an overly formal and cumbersome approach.

I have no objections.

Attachment

PLEASE RETURN
TO JOHN'S FILES.

THE WHITE HOUSE

WASHINGTON

November 17, 1983

MEMORANDUM FOR GREGORY JONES
LEGISLATIVE ATTORNEY
OFFICE OF MANAGEMENT AND BUDGET

FROM: FRED F. FIELDING Orig. signed by FFF
COUNSEL TO THE PRESIDENT

SUBJECT: Statement of John C. Keeney
Re: Computer Crime -- H.R. 1092
on November 18, 1983

Counsel's Office has reviewed the above-referenced testimony, and finds no objection to it from a legal perspective.

FFF:JGR:aea 11/17/83
cc: FFFielding/JGRoberts/Subj/Chron

THE WHITE HOUSE

WASHINGTON

November 17, 1983

MEMORANDUM FOR GREGORY JONES
LEGISLATIVE ATTORNEY
OFFICE OF MANAGEMENT AND BUDGET

FROM: FRED F. FIELDING
COUNSEL TO THE PRESIDENT

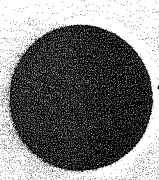
SUBJECT: Statement of John C. Keeney
Re: Computer Crime -- H.R. 1092
on November 18, 1983

Counsel's Office has reviewed the above-referenced testimony, and finds no objection to it from a legal perspective.

FFF:JGR:aea 11/17/83
cc: FFFielding/JGRoberts/Subj/Chron

ID # _____ CU

WHITE HOUSE
CORRESPONDENCE TRACKING WORKSHEET



John

☐ O - OUTGOING
☐ H - INTERNAL
☐ I - INCOMING
Date Correspondence Received (YY/MM/DD) 1 1

Name of Correspondent: Greg Jones

☐ **MI Mail Report** **User Codes: (A)** _____ **(B)** _____ **(C)** _____

Subject: Statement of John C Keeney re: Computer Crime H.R. 1092 on November 18, 1983

ROUTE TO:		ACTION		DISPOSITION		
Office/Agency	(Staff Name)	Action Code	Tracking Date YY/MM/DD	Type of Response	Code	Completion Date YY/MM/DD
CUHOLL		ORIGINATOR	83/11/16			/ /
		Referral Note:				
CUAT18		D	83/11/16		S	83/11/18
		Referral Note:				
			/ /			/ /
		Referral Note:				
			/ /			/ /
		Referral Note:				
			/ /			/ /
		Referral Note:				

ACTION CODES:
A - Appropriate Action
C - Comment/Recommendation
D - Draft Response
F - Furnish Fact Sheet to be used as Enclosure
I - Info Copy Only/No Action Necessary
R - Direct Reply w/Copy
S - For Signature
X - Interim Reply

DISPOSITION CODES:
A - Answered
B - Non-Special Referral
C - Completed
S - Suspended

FOR OUTGOING CORRESPONDENCE:
Type of Response = Initials of Signer
Code = "A"
Completion Date = Date of Outgoing

Comments: _____

Keep this worksheet attached to the original incoming letter.
Send all routing updates to Central Reference (Room 75, OEOB).
Always return completed correspondence record to Central Files.
Refer questions about the correspondence tracking system to Central Reference, ext. 2590.

5/81

DRAFT

STATEMENT

OF

JOHN C. KEENEY
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE

THE

SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

CONCERNING

COMPUTER CRIME - H.R. 1092

ON

NOVEMBER 18, 1983

Mr. Chairman and Members of the Subcommittee, it is a pleasure to be here today to help present the views of the Department of Justice in regard to computer fraud and related topics.

I would note initially that, as you are no doubt aware. there is currently no sanction available specifically dealing with computer-related crime. Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a "theory of prosecution" that somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets. The crafting of such a theory can be awkward, and the results far from perfect. Even if a theory is devised that apparently covers the illegal acts, it still must be treated as an untested, untried basis of prosecution in the trial court. This could lead to the dismissal of a prosecution, notwithstanding the egregious nature of the crime or the extensiveness of trial preparation, because decades old statutory elements designed to deal with other crimes have been stretched too far to accommodate modern criminality. Mr. Chairman, let me give you some examples of the difficulties that can arise in trying to prosecute computer-related crime under existing statutes.

Three well known cases, all of which were unreported, present themselves. In the Seidlitz case, a federal wire fraud case tried in Maryland, the owner of a computer company stole confidential software by tapping into the computer system of a previous employer from his remote terminal. Had the defendant not made two of the fifty access calls across state lines, there would have been no basis for federal prosecution. Only a state statute on theft of trade secrets would have remained as a possible recourse.

In the Langevin case, another case involving a violation of the federal wire fraud statute in which the defendant eventually pleaded guilty in the District of Columbia, a former employee of the Federal Reserve Board who was then employed privately as a financial analyst was apprehended after he attempted to continue to access information in the Federal Reserve Board's money supply (M-1) file without authorization. Any information he might have obtained would have been extremely useful in analyzing his client's holdings. As in Seidlitz, had the access telephone calls not gone across state lines, we would not have been able to use the wire fraud statute and would have had to prosecute the defendant for theft of government property, i.e. the information. Fixing a value on the information, a necessary element of proof, would have been very difficult.

In the Rivkin case, a computer expert fraudulently used a bank's in-house access codes to transfer millions of dollars to accounts he controlled in another bank. As it turned out, the

defendant was prosecuted in the California state court system. However, the facts of the case point up the potential gaps in the current laws that may be present in any case in which federal prosecution is considered. If the wire communications transferring the funds had all been in the same state there is no apparent theory under which federal prosecution could have been undertaken.

Turning to the three bills presently before the Subcommittee, all of them attempt to close the potential gaps that exist in the present law that could negate present federal statutes. As you probably know, the Administration is actively reviewing various legislative proposals in this area but at this juncture we have not yet reached a final decision on what type of new legislation we believe is needed. We hope to send a recommendation to the Congress in the near future.

In that context, let me give some very preliminary comments on the three bills before you. H.R. 1092 would criminalize a number of acts committed upon, or by means of, various computers. This approach is one which we are carefully considering, along with other concepts not in H.R. 1092 such as a misdemeanor for simple unauthorized access to computers in which there is a particular federal interest. Moreover, if we ultimately support the approach of H.R. 1092 we would probably recommend that it be slightly redrafted to track the present mail and wire fraud statutes, 18 U.S.C. 1341 and 1343, respectively. These statutes have beem interpreted in literally hundreds of cases and the

adaptation of the same language would ensure that the new statute would cover virtually any type of fraud scheme using the designated computers.

As for H.R. 4021, while we are still studying all options, at this point we believe that the approach incorporated in bills such as H.R. 1092 is preferable to creating what is essentially an enhanced penalty section in title 18 for crimes committed with computers.[1]

Turning finally to H.R. 4259, the bill has four titles. I would authorize the Secretary of Commerce to make grants to private persons for the purpose of developing new methods of protecting computer systems from unauthorized access and use. While such a program might be beneficial, we would prefer to wait until the Administration is able to take a final position with respect to the need for new legislation in this area to comment on the need for such a program and, in any event, we would defer to the Commerce Department as to the feasibility of a grant program in this area.

Title II would create a Federal Interagency Committee on Computer Fraud and Abuse which would be chaired by the Attorney General. The Committee would perform various functions such as compiling and disseminating statistics on computer fraud and

---

[1] While we realize that 18 U.S.C. 924(c) concerning the use of a firearm in a federal crime, on which H.R. 4021 is based, has been interpreted as creating a distinct offense and not as an enhanced penalty provision, H.R. 4021 would still require the proof of all of the elements of some other federal crime and thus would not help in filling potential gaps in the coverage of existing statutes.

coordinating the development of more secure computer systems for the federal government. It would also make recommendations on improving the security of federal computers and on the need for new legislation. We do not believe that it is necessary to establish the somewhat cumbersome vehicle of a formal interagency committee to accomplish these tasks. While laudatory, they can be carried out by much less formal means of coordination and consultation. For example, I mentioned earlier that the Justice Department is presently studying the need for additional legislation that would criminalize the use of a computer in fraud scheme and a provision making it a crime to access a computer without authority. Before being adopted, any such proposal will be discussed with all other interested agencies in the course of the normal OMB review process.

Title III is very similar in substance to H.R. 1092, and my comments on that bill are equally applicable here.

As for Title IV, which provides for tax credits for persons who purchase certain home computers, this is a matter on which the Department of Justice would defer to the Treasury Department.

Mr. Chairman, that concludes my prepared testimony and I would be happy to attempt to answer any questions that the Subcommittee may have.