THE WHITE HOUSE

WASHINGTON

October 13, 1983

MEMORANDUM FOR FRED F. FIELDING

FROM: JOHN G. ROBERTS

SUBJECT: Statement of John C. Keeney Regarding Credit Card Fraud on October 17, 1983

We have been provided with a copy of the statement Deputy Assistant Attorney General John C. Keeney proposes to deliver on October 17 before the Senate Judiciary Committee. The proposed testimony presents the views of the Department of Justice on S. 1870, a bill that would provide criminal penalities for certain credit and debit card counterfeiting and related fraud. The testimony supports the thrust of the bill, but suggests several substantial revisions to respond to specific problems that the Department has encountered in prosecuting this type of fraud. The testimony also suggests that the Committee consider amending Title 15, the current home of the Truth-in-Lending and Electronic Funds Transfer Acts, rather than Title 18 to address these problems. Finally, the testimony urges the Committee to enact Part G of Title XI of S. 1762, the Comprehensive Crime Control Act of 1983, as part of its effort to fill in the gaps in the present law regarding bank fraud. I have reviewed the testimony and have no objections to it.

Attachment

THE WHITE HOUSE

WASHINGTON

October 13, 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
Regarding Credit Card Fraud on
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 10/13/83

cc: FFFielding
JGRoberts
Subj
Chron

JV

ID # 178890 CU

JN023

Peter handled

WHITE HOUSE
CORRESPONDENCE TRACKING WORKSHEET

☐ 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: Credit Card Fraud on 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
CUHOLL	ORIGINATOR	83/10/12		_	1 1
CWAT 18	Referral Note: DD				
	D DD	83/10/12		S	83/10/14
	Referral Note:				
	_	1 1		_	1 1
	Referral Note:				
	_	1 1		_	1 1
	Referral Note:				
	_	1 1		_	1 1
	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: See 143398CU - FYI only DD

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

178890

OF

JOHN C. KEENEY
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE

THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

CREDIT CARD FRAUD

ON

OCTOBER 17, 1983

Mr. Chairman and Members of the Committee, I am pleased to be here today to present the views of the Department of Justice on S. 1870, a bill to provide penalties for credit and debit card counterfeiting and related fraud. The Department strongly supports the concept of this bill, but we will suggest certain substantial modifications.

Before discussing the specifics of S. 1870, I think it would be useful to describe for the Committee 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 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 Electronic Fund Transfers (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 where 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 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

---

[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.

[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).

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.

In our view, S. 1870 sufficiently covers the counterfeiting of credit and debit cards. However, it only partially overcomes 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, and does very little to overcome 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

---

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.

violating the statute. These strengths and weaknesses of S. 1870 can better be understood by an examination of the various parts of the new section 1029 which the bill would add to title 18.

Subsection 1029(a)(1) would cover such acts as counterfeiting a credit or debit card with intent to defraud, and selling, transferring or buying an altered, lost, or stolen credit card or card number with fraudulent intent. It would also overcome some of the problems pointed up by the Kasper case whereby the present credit card fraud statute does not cover the situation in which a person uses a credit card that he had been given by, or that he had bought from, the person to whom it was legimitately issued for the purpose of charging goods without paying for them, and the card is then reported lost by the original cardholder. It does this through its proscription of buying, selling, or transferring a "fraudulent payment device," a term defined in subsection 1029(d) as a credit or debit card or card number "that is counterfeit, fictitious, altered, forged, lost, stolen, incomplete, fraudulently obtained or obtained as part of a scheme to defraud." Interestingly, 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 by the subsection. Moreover, the subsection would not directly cover a person who obtained a card for no consideration as part of such a plan,[4]

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

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.

The new subsection 1029(a)(3) would complement the proscription of card counterfeiting in 1029(a)(1) by prohibiting the producing, buying, selling, transferring or having control, custody, or possession of equipment for making a fictitious, altered, forged, or incomplete credit or debit card. Subsection 1029(a)(2) would prohibit the possessing or controlling, with intent to defraud or transfer unlawfully, five or more counterfeit, fictitious, altered, forged, lost, stolen, incomplete or fraudulently obtained credit or debit cards or card numbers.

The new section attempts to cover misuse of card numbers by defining the term "payment device" in subsection 1029(d)(1) to include account numbers. Thus, the proscription in 1029(a)(1) of producing, buying, selling, or transferring a fraudulent payment device with intent to defraud would cover the buying, selling, or transferring of a fraudulent card number. However, neither 1029(a)(1) nor any other portion of the new section would cover the actual use of the card number, for example, by a person who gave a fictitious number or the number on someone else's card to order goods over the telephone.[5] While to be sure 1029(a)(1) would cover the conduct of the dishonest bank or store employee who sold or transferred a person's card number to another person

---

[5] Making up a number, or using someone else's, would not be covered by the term "produce" since produce is defined in 1029(d)(3) as "to make, design, alter, authenticate, duplicate, or assemble."

so that he could use it to charge goods without authority, and would also cover the person who bought such a number, the lack of proscription of the actual use of the number seems an unjustifiable gap in the proposed statute. Although it may be that the drafters of the bill intend that the concept of "use" of the number be included in the term "transfer," this certainly is not apparent from the context and needs clarification.

The new section is, in our view, also deficient in not overcoming the so called accumulation problem which is caused by the wording of 15 U.S.C. 1644(a), which currently provides:

> "Whoever 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 or more".

15 U.S.C. 1693n(b)(1) tracks this language for debit cards. Our experience has indicated that certain persons make a practice of evading this statute by carefully charging less than $1,000 on any one improperly obtained card and then doing the same thing with other such cards. This is an obvious deficiency in the present law that should be addressed. While subsections 1029(a)(2), which prohibits possession with fraudulent intent of five or more fraudulent payment devices, and 1029(a)(1), which prohibits the buying of a fraudulent card, might reach some of these career credit card criminals, these provisions would only

be of use if it could be proven beyond a reasonable doubt that the person had possession, custody or control of five or more cards simultaneously, or had bought one of the cards, as opposed to having received it as a gift or having stolen it.

In sum, although the bill is a good first step toward resolving present inadequacies in the federal statutes punishing credit and debit card fraud, we believe it needs considerable refinement to adequately treat the problems discussed above, with the exception of its coverage of counterfeiting of cards. Moreover, we are troubled by the fact that the bill take the approach of only amending title 18 to add a new series of offenses while leaving intact the current title 15 statutes. This means that, if S. 1870 were to be enacted, we would be left with the unusual situation whereby coverage of unlawful acts involving credit and debit cards is split confusingly between titles 15 and 18. While we recognize that this approach may have been dictated in part by the belief of some representatives of the bank card industry that offenses in title 18 are more likely to be prosecuted than those set out elsewhere, and by considerations of this Committee's jurisdiction, we believe that the Committee should consider amending the title 15 statutes themselves as well, possibly by seeking a sequential referral of the bill to another committee, as a more effective way of combating most types of credit and debit card crimes.

In fact, Mr. Chairman, as you may know, the Subcommittee on Consumer Affairs of the Committee on Banking, Housing and Urban Affairs has already held a hearing on credit card fraud. Subsequent to testimony by representatives of the Department of Justice at that hearing, we furnished draft legislation amending the Truth in Lending Act and the EFT Act to overcome the problems of their lack of coverage of card numbers, the accumulation issue, and the problems caused by the "fraudulently obtained" language as construed in Kasper. We have concluded that these issues can best be resolved by amending the Truth in Lending and EFT Acts.

While counterfeiting or altering of cards could appropriately be addressed separately in title 18, in order to avoid confusion and inconsistency between the title 18 and title 15 offenses we would suggest that the description of the device counterfeited or altered be set out by cross-reference to the 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 necessity of introducing the new term "payment device" into the law. While the phrase may be a term of art in the credit and debit card industry, such a novel term may unnecessarily complicate criminal prosecutions. We would, of course, be happy to work with the Committee to prepare language covering counterfeiting for inclusion in title 18.

Moreover, to the extent that the Committee is generally reviewing the ability of the federal government to investigate and prosecute fraud against financial institutions and other

credit and debit card issuers, it should in our view strongly consider including in this bill the provisions of Part G of Title XI of S. 1762, the Comprehensive Crime Control Act of 1983, as recently reported out by the Committee. Present laws designed to protect banks cover the offenses of embezzlement, robbery, larceny, burglary, and false statements. Part G is designed to fill the gaps in the present law regarding defrauding banks. It is modeled on the present mail and wire fraud statutes and proscribes a scheme or artifice to defraud a federally chartered or insured financial institution or to obtain property owned or under the control or custody of such an institution by means of false or fraudulent pretenses, representations, or promises. The proposed offense would clearly cover fraudulent schemes involving credit or debit cards in which a federally insured bank is victimized. Inclusion would thus complement the credit card offense provisions.

In conclusion, Mr. Chairman, while we strongly support the thrust of this legislation, we believe that the present deficiencies in the credit and debit card crime area, with the exception of the counterfeiting of cards, can be most effectively addressed by amending the Truth in Lending and EFT Acts. While card counterfeiting could be covered in title 18, the provisions in the present bill should be modified to include definitions in the Truth in Lending and EFT Acts, and we would recommend the inclusion of the bank fraud provisions of S. 1762 in any legislation in this area.

Mr. Chairman, that concludes my prepared statement and I would be happy to try to answer any questions that the Committee may have.

THE WHITE HOUSE

WASHINGTON

October 19, 1983

MEMORANDUM FOR FRED F. FIELDING

FROM: JOHN G. ROBERTS JGR

SUBJECT: Statement of Conrad S. Banner Regarding Federal Identification Systems on October 21, 1983

OMB has provided us with a copy of the testimony Conrad Banner, Deputy Assistant Director of the FBI's Identification Division, proposes to deliver on October 21 before the Subcommittee on Courts of the Senate Judiciary Committee. The testimony begins with an overview of the FBI's Identification Division, with which you are of course familiar, and the National Crime Information Center, which contains a wide variety of criminal histories and related data. The bulk of the testimony discusses various methods of identification, in particular fingerprints, and the advantages and disadvantages of each type. The testimony concludes with a general discussion of security and privacy considerations in the use of identification systems. I have reviewed the testimony and have no objections to it.

Attachment

THE WHITE HOUSE

WASHINGTON

October 19, 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: Statement of Conrad S. Banner Regarding Federal Identification Systems on October 21, 1983

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

FFF:JGR:aea 10/19/83

cc: FFFielding
JGRoberts
Subj
Chron

ID # _____ CU

WHITE HOUSE
CORRESPONDENCE TRACKING WORKSHEET

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

Name of Correspondent: Branden Blum

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

Subject: Statement of Conrad S. Banner re: Federal Identification Systems on October 21, 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
CU	DOLL	ORIGINATOR	83/10/19			/ /
		Referral Note:				
CUAT	18	D	83/10/19		S	83/10/20
		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

OPENING STATEMENT

OF

INSPECTOR CONRAD S. BANNER

DEPUTY ASSISTANT DIRECTOR, IDENTIFICATION DIVISION

FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON COURTS

JUDICIARY COMMITTEE

UNITED STATES SENATE

ON

OCTOBER 21, 1983

REGARDING

FEDERAL IDENTIFICATION SYSTEMS

Mr. Chairman and Members of the Subcommittee:

I am Inspector Conrad S. Banner, the Deputy Assistant Director (Operations) of the FBI's Identification Division. Accompanying me is Section Chief David F. Nemecek, the head of the FBI's National Crime Information Center (NCIC) Section. We are here today at the Chairman's invitation to provide information regarding the FBI's experience in operating the Nation's two largest criminal justice information systems, namely the FBI Identification Division and the NCIC.

Perhaps a brief description of these two systems would be appropriate at this juncture:

FBI Identification Division

The FBI's Identification Division was established by an Act of Congress in 1924, at the urging of the International Association of Chiefs of Police. Two developments at the turn of the century were instrumental in the Division's creation. The first was the adoption by criminal justice authorities of the use of fingerprints as a positive means of identifying criminals. The second was the increasing mobility of criminals. Efficiency and economy made it imperative that there be a national index where a single inquiry could be made to determine whether a person had a prior criminal record, rather than having to poll each of the numerous criminal justice jurisdictions throughout the United States to make that determination.

The Identification Division operates in the following manner: Federal, state and local criminal justice agencies mail in arrest fingerprint cards and disposition reports, which the Division uses to compile its criminal history records. Inquiries regarding these records are received in the form of arrest and applicant fingerprint cards and name-checks, which are mostly submitted and

responded to through the mail. The Division also acts as the national repository for fingerprint cards taken in connection with employment in the Federal Government, service in the U. S. armed forces, alien registration, and personal identification, including missing persons and unidentified deceased persons. As of September 1, 1983, the Division's fingerprint card holdings totaled 172.8 million cards, including 81.5 million criminal cards relating to 21.7 million persons, and 91.3 million civil cards relating to 43.3 million persons. Additional services provided by the Identification Division are: (a) the posting of wanted, probation/parole, and other notices in its files for criminal justice agencies so that appropriate authorities can be notified of subsequent criminal activity by the subjects of the records; (b) the processing of physical evidence for latent "crime scene" finger and palm prints, and the furnishing of expert court testimony as to the findings; (c) the training of law enforcement personnel in fingerprint science; and (d) assisting federal, state and local authorities in the identification of unknown amnesia and disaster victims. The Identification Division presently services over 19,000 authorized users.

National Crime Information Center (NCIC)

The NCIC system was established in 1967. It is a computerized information system containing data on wanted persons, missing persons, unidentified persons, stolen property, criminal histories, and firearms identification. The NCIC was developed as the result of a cooperative effort by federal, state and local criminal justice agencies to make information vital to their operations available instantaneously. These agencies are able to enter information into the NCIC system where it is available for on-line retrieval through computer terminals located in criminal justice agencies throughout the United States.

When the NCIC system became operational in 1967, it contained an Article File, a Gun File, a License Plate File, a Vehicle File, and a Wanted Person File. The following files were subsequently added: a Securities File in 1968; a Boat File in 1969; a Computerized Criminal History (CCH) File in 1971; a Missing Person File in 1975; a Firearms Rifling Characteristics File in 1978; a Canadian Warrants File in 1980; and in 1983 an Interstate Identification Index (Triple-I) File (which replaced the CCH File), a U. S. Secret Service Protective File, and an Unidentified Person File. As of September 1, 1983, there were 15,791,446 records in the NCIC data base, broken down as follows: 1,347,600 stolen article records; 25,747 stolen boat records; 289 Canadian warrant records; 14,309 firearms rifling characteristics records; 1,883,910 stolen and recovered gun records; 579,303 stolen license plates records; 88 U. S. Secret Service Protective records; 2,464,396 stolen securities records; 8,026,987 Triple-I records; 1,244,088 stolen vehicle, felony vehicle, and vehicle part records; and 204,729 wanted person records. An estimated 22,000 user terminals utilized the NCIC system for an average of 412,635 transactions each day during September 1983.

General Comments

I note that Mr. Gary D. McAlvey, Chief of the Illinois Bureau of Identification, and a past Chairman and present Member of the Board of Directors of SEARCH Group, Inc., testified before this Subcommittee on July 29, 1983. In his testimony, Mr. McAlvey focused on: (1) the highly successful efforts of the criminal justice community in achieving standardization of the data elements utilized in federal, state and local criminal justice information systems; (2) the use of fingerprints by criminal justice practitioners as a positive

means of identification; and (3) the security and privacy aspects of operating criminal justice information systems.

In order to conserve the Subcommittee's valuable time, I shall not attempt to duplicate here the information Mr. McAlvey furnished in his testimony. Rather, I shall only attempt to supplement that testimony with my own views and insights.

Standardization of Data Elements and Formats

In regard to standardizing data elements and formats, I believe the lessons learned in the criminal justice sector are both germane and encouraging. As Mr. McAlvey indicated, the criminal justice community has been able to achieve a high degree of standardization in the data elements and formats used in its information systems. If this can be done among the numerous and diverse federal, state and local information systems scattered around the country, it would appear to be more easily and more completely achievable in a situation where the information systems are operated under the aegis of a single sovereign -- i.e., the Federal Government.

Positive Identification

There is an increasing variety of ways to identify people -- e.g., fingerprints, footprints, lip prints, voice prints, hand dimensions, retina scanning, dental characteristics, blood analysis, etc. But, the most practical and universally accepted means is fingerprints. Up until now, the criminal justice community has been the major user of fingerprints. Recognizing the dire consequences to a person falsely accused of a crime, criminal justice practitioners adopted fingerprints as a positive means of identifying people

and linking them to their criminal records. The FBI's Identification Division represents a system which bases its entire existence and operational integrity on its ability to positively identify individuals by their fingerprints. To illustrate, before a criminal record is initially established in the Division's files, a fingerprint search is conducted to insure that there is no record already on file for the person under a different name. Also, before each subsequent arrest entry is added to the record, a fingerprint comparison is performed to insure that the new arrest truly relates to the existing record. Finally, before the Division will respond to an inquiry as to whether there is, or is not, a record on file for a person, the Division requires that the person's fingerprints be submitted and searched. This insures that the person's record is not missed because of his/her use of another name, and that any record which is located truly relates to the person who is the subject of the inquiry. While the Identification Division does accept name check inquiries, any criminal record sent out in response contains a caveat stating that, since it is not being disseminated on the basis of a fingerprint comparison, no guarantee can be given that the record relates to the subject of the inquiry.

The NCIC system is, on the other hand, a computerized "name and number" searching system. Many items of personal property — e.g., automobiles, television sets, guns, etc. — have a unique manufacturer's serial number engraved on, or otherwise permanently affixed to, them. If not altered or obliterated, these numbers provide a positive means of identifying the property. Such numbers are well suited for storage and retrieval of records in a computerized system such as the NCIC.

Problems arise when dealing with people, as they normally do not have serial numbers indelibly marked on them. When a person is not known to

criminal justice authorities, reliance must be placed on the name and other personal information orally furnished by the person, and/or that available in identification documents provided by the person. However, the name, personal information (e.g., date and place of birth), and identification documents (e.g., driver's license) which are available may all be fictitious, thereby frustrating a computerized name and number search. This does not mean that name and number searches on people are useless. To the contrary, our experience in the criminal justice field has proven that they are productive in most instances. This is because most people readily admit their true identities. Furthermore, in many instances the authorities already know the true identity of the person.

Even when people admit their true identities, the names and numbers they provide have varying effectiveness for file searching. The selectivity and reliability of names and numbers depend on the unusualness of the names and the uniqueness of the numbers.

The least effective name and number search is one using name and date of birth. Many people have the same or a similar name, and many people have the same date of birth. In the case of a common name, such as Smith or Jones, the search may produce so many possible matching records that it is impossible to determine the correct record.

Numbers such as a person's driver's license number, military service number, or Social Security Number, provide a more positive means of retrieving the correct record. However, there are problems in the use of such numbers. Our experience has shown that they are not necessarily unique, since some duplicates have been found. Furthermore, because they are long numbers, they are prone to be incorrectly recorded. Incorrect recording can be detected by a

computer system if "self-checking" digits are added to the numbers. The self-checking digits are derived from the base number by a computer using a mathematical formula. Whenever the number is again entered into the computer, the same mathematical formula is used to recompute the check digits and the result is compared with the check digits on the original number. If the newly computed check digits do not equal those on the original number, an error condition is signaled. The use of self-checking FBI Numbers in the NCIC system and in the Identification Division's automated files has proven to be effective in minimizing the adverse impact of errors in recording FBI Numbers.

The 20-digit NCIC fingerprint classification provides a highly selective means of locating records in a computerized file. It is not, however, a positive means since more than one person can have the same fingerprint classification. Another disadvantage is that it requires a trained fingerprint technician to derive the classification.

Selectivity in file searching can be improved through the use of additional descriptors. For example, the use of not only name and date of birth, but also sex, race, height, weight, and eye and hair color, can increase the chances of retrieving the correct record, particularly when the descriptors are verifiable through personal observation of the subject. However, there is a danger in being too selective. The descriptors used for file searching may not correspond with those on file because of: earlier recordation errors (e.g., the person's height is 6 feet 4 inches but was recorded as 64 inches); differences in people's powers of observation (e.g., "hazel" versus "brown" eyes); and/or actual changes in the subject's appearance (e.g., his hair is now gray and he weighs more). Requiring exact matches on such descriptors could result in missed identifications. Therefore, the Identification Division has developed elaborate scoring (weighting) schemes to avoid these types of misses.

Factors Bearing on the Type of Identification Method that Should be Used

Mr. McAlvey pointed out that the purpose of an identification system should have a bearing on the searching method to be used. I agree. There are two basic purposes: (1) to "verify" a person's identity; or (2) to "identify" the person. In a verification situation — e.g., where the person must prove his/her identity in order to receive a benefit such as food stamps — the amount of searching can be limited to comparing the identification information provided by the person against that on file for the person he/she claims to be. If the comparison is negative, the identification process can be concluded with the person being denied the benefit until he/she is able to produce better proof of identity. It would appear that in the verification situation, the use of an alteration-resistant identification document bearing the person's name, physical description, a self-checking identification number, and the person's photograph and/or fingerprint, would be sufficient to prevent most fraudulent claims. On the other hand, in an identification situation, it is usually in the person's best interest not to cooperate in proving his/her true identity as to do so would be detrimental to the person, e.g., the National Driver Registry. Therefore, file searching should not be ended just because the identification information furnished by the person fails to match a record on file. The search should continue, using some means of identification which is independent of the person's cooperation, such as fingerprints.

The amount of time required to perform a particular type of file search and its intrusiveness to the individual are also factors which should have a bearing on the searching method to be used. For example, the use of fingerprints is both time-consuming and intrusive. Most fingerprints are taken using printer's ink and a card. The inked impressions must be taken by someone

trained in the proper procedure or they may be unsuitable for searching purposes. The procedure is unpleasant for the person being fingerprinted since his/her hands become soiled. It takes a skilled technician or expensive automated equipment to perform fingerprint searches, and the entire procedure usually takes days or weeks. So, while fingerprinting may be a suitable procedure when dealing with an arrestee or a person applying for employment or a license, it would not be suitable for conducting routine motor vehicle traffic checks.

Cost is, of course, another important factor. A "name and number" search of the NCIC system costs a little less than five cents, while a fingerprint search by the FBI's Identification Division costs $12.

Finally, the availablity of identifying data may be a determining factor in regard to the type of searching method that can be used. There are situations where the individual is unable to orally provide identifying information and there are no identification documents on his/her person. These situations typically involve unknown deceased persons, amnesia victims, or very young children. If known fingerprints are available for the person, they can be used to accomplish the identification. On the other hand, if known fingerprints are not available, or the condition of the person's body precludes fingerprint comparisons, then other methods of identification must be attempted.

An Unidentified Person File was recently added to the NCIC system. It is designed to search physical descriptive information (e.g., age, sex, race, height, weight, hair color, eye color, scars, marks, tattoos, missing and/or artificial body parts, dental characteristics, etc.), and information regarding clothing and personal effects (e.g., jewelry). While these types of data elements have previously been used in manual and off-line "batch" computer

searches to help identify unknown persons, it appears that the NCIC's Unidentified Person File is the first application of on-line computer searching techniques to the problem. The NCIC's Missing Person File is being reprogrammed so that it too will not require a unique numerical identifier, such as date of birth or Social Security Number, for searching. This change is necessary in order to provide a means of identifying very young children who do not know their date of birth, and do not have a Social Security Number or other identification number. The effectiveness of using nonunique descriptors to conduct on-line searches of NCIC is yet to be determined.

Security and Privacy

I shall not dwell on the need for any information system containing personal information to have adequate security safeguards to prevent unauthorized access and misuse of the information. This is self-evident. The criminal justice community has been successful in establishing adequate physical and programmatic safeguards for its information systems. It has not been as successful in agreeing on who should have access to those systems. While there is no disagreement regarding access by criminal justice agencies, there is wide disagreement among the states regarding access by noncriminal justice employment and licensing authorities. Some states have policies forbidding access for employment and licensing purposes, while other states have policies allowing access for any purpose. Most states have adopted policies lying somewhere between these two extremes. This leads me to the area of privacy, since it is the root cause of the disagreement over access.

Any initiative to standardize, combine, or link Federal Government information systems, and/or establish a national system for identifying persons, will inevitably give rise to privacy concerns. Therefore, privacy concerns

should be addressed as an integral part of the deliberations and planning for any such initiative. The planners must strike the difficult balance between the Government's legitimate need to identity and maintain information about people and their right to privacy.

The task is made simpler when the Government bestows a benefit. Most people are willing to give up some amount of privacy in order to reap a reward. This principle has been used extensively in the employment and licensing area. People applying for Federal Government employment, service in the U.S. armed forces, naturalization as a U.S. citizen, and/or access to classified material, are fingerprinted and their prints are searched through the FBI's criminal fingerprint file to determine whether they have arrest records. Similarly, many states have passed laws requiring a check of the FBI's criminal fingerprint file on persons applying for employment or licenses in activities involving public safety. The most pervasive use of this principle is in the area of operating motor vehicles. In exchange for the privilege of operating a motor vehicle within a state, a person must obtain, and carry on his/her person, a valid driver's license. The license contains the person's name, address, physical description, and in many states the person's photograph. State driver's licenses are so well accepted as identification documents that they have become de facto identification cards for many purposes other than driving. While the principle of giving up some amount of privacy for a benefit is well established and generally undisputed, it is very questionable whether most Americans would willingly allow incursions into their privacy without a promised benefit.

Although I have advocated the use of fingerprints as the most practical and universally accepted means of positively identifying people, fingerprinting does arouse some privacy concerns. Since the criminal justice

community has been the primary user of fingerprints up to now, the procedure has acquired the connotation of criminality. During the 1970's when authorities were looking for a positive means of identifying people enrolled in drug treatment programs, the use of fingerprints was rejected in lieu of footprints as it was believed that the enrollees would be reluctant to submit to fingerprinting. In order to remove possible privacy concerns in fingerprinting children participating in missing children programs, the FBI has recommended that the child's parents or guardian decide whether a child will, or will not, be fingerprinted; and, if it is decided that the child will be fingerprinted, that the child's fingerprint card be retained by the parents or guardian until it is needed. Only then, would the card be furnished to law enforcement authorities to assist them in locating the child. I believe that, with time and wider usage of fingerprints for noncriminal justice purposes, these types of concerns will eventually be dispelled.

Conclusion

Mr. Chairman, this concludes my prepared statement. I hope that the information furnished will be of assistance to the Subcommittee. Mr. Nemecek and I would now be pleased to respond to the Subcommittee's questions.

THE WHITE HOUSE

WASHINGTON

October 19, 1983

MEMORANDUM FOR FRED F. FIELDING

FROM: JOHN G. ROBERTS

SUBJECT: Statement of Roger P. Brandemuehl Regarding Federal Identification Systems and Fraudulent Use of Identification Documents - 10/21/83

OMB has provided us with a copy of the proposed testimony of Roger P. Brandemuehl, Acting Associate Commissioner of INS, which is to be delivered before the Subcommittee on Courts of the Senate Judiciary Committee on October 21. The testimony reviews the various documents issued by INS which may be used for identification purposes, and examines the rising problem of counterfeiting identifiers for the purpose of obtaining citizenship and the benefits accruing thereto. In particular, the testimony describes how an individual obtaining one key identification document, called a "breeder document," can use that document to secure a broad range of other identification documents. The testimony reviews several efforts to combat this problem, including the establishment of task forces across the country. I have reviewed the testimony and have no objection to it, although, for the sake of any members of the Subcommittee who may be in attendance, I hope that Mr. Brandemuehl is a fast reader.

Attachment

THE WHITE HOUSE

WASHINGTON

October 19, 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: Statement of Roger P. Brandemuehl Regarding Federal Identification Systems and Fraudulent Use of Identification Documents - 10/21/83

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

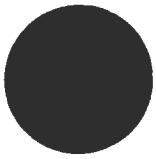
FFF:JGR:aea 10/19/83

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: Brander Blum

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

Subject: Statement of Roger P. Brandemuehl re: federal identification systems and fraudulent use of identification documents October 21, 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	83/10/18			/ /
	Referral Note:				
CUAT 18	D	83/10/18		S	83/10/20
	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

ROGER P. BRANDEMUEHL
ACTING ASSOCIATE COMMISSIONER,
ENFORCEMENT
U.S. IMMIGRATION AND NATURALIZATION SERVICE

BEFORE THE SUBCOMMITTEE ON COURTS
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
OCTOBER 21, 1983

Mr. Chairman and members of the Subcommittee:

On behalf of the Immigration and Naturalization Service, I am pleased to have this opportunity to testify on federal identification systems, and, in particular, about our efforts to counter the fraudulent use of identification documents.

INS INVOLVEMENT IN FEDERAL IDENTIFICATION

The Service issues seven major types of identification cards and registration documents which are used as identifiers: the I-551 Alien Registration Receipt Card, the I-586 Nonresident Alien Mexican Border Crossing Card, the Haitian Identification Card, the I-94 Arrival-Departure Record, the I-95A Crewman's Landing Permit, Certificates of Naturalization, and Certificates of Citizenship. These forms are used to identify permanent resident aliens and United States citizens, and to register nonimmigrant aliens. The documents serve both as permanent identification for certain U.S. citizens and lawful permanent resident aliens, and as evidence of lawful temporary admission for nonimmigrant aliens. Approximately thirteen million I-94's and one million other documents are issued each year.

Beginning in 1940, identification cards were issued by the Service to lawfuly admitted resident aliens. These cards contained some security features, and new versions were issued over the years with new features to enhance security. Eventually, seventeen versions of the Alien Registration Receipt Card, Form I-151, commonly called the "green card," were issued by INS. The I-151 was rather easily counterfeited, altered, or used by imposters, so in 1975 the Service decided to produce a more reliable identification card, backed by a secure computer system. The Alien Documentation, Identification and Telecommunications (ADIT) Program was funded in Fiscal Year 1976 to develop a secure document system for the Service. The card issuance segment of the system became operational in March 1977.

Production of the secure ADIT I-551, Alien Registration Receipt Card, and I-586, Nonresident Alien Border Crossing Card, consists of processing card applications received from Department of State consulates and INS field offices, fabricating the cards, generating the corresponding central data record of card issuance, and delivering the card to the lawful holder. Card production is accomplished at the Immigration Card Facility (ICF), located at Grand Prairie, Texas. That facility is operated under contract, with on-site quality control and performance monitoring by INS employees. Production and delivery of the card to the alien satisfies the INS statutory responsibility to issue cards to permanent resident aliens and nonresident alien border crossers.

This automated system provides capability for access, via remote terminals, to central computer-stored data pertinent to the inspection of INS issued identification cards and individuals presenting them. Video terminal inquiry facilities are currently installed at all district offices as well as the secondary inspection units at major air and land ports of entry.

As envisioned, the integration of the three components of the ADIT system--accurate data collection, quality card production, and automated verification--are necessary to insure its security. Identification can generally be achieved solely by examining a card. However, positive verification can only be achieved by accessing the on-line ADIT computer records, which provide examiners with accurate information on the identification and current status of the card and its lawful holder.

The ADIT Program developed a system which has proven effective. To date, approximately 4 million high quality cards have been produced and issued. The I-551 and I-586 cards are produced at the centralized facility, so that standardization has been maintained. Personal identifiers in this ADIT card system consist of the individual's name, date of birth, fingerprint, color photograph, and signature. Administrative data consisting of an assigned alien identification number, port of entry, and

class of admission are also included in the system. Document security features begin with the artwork of the form itself, include coded personal biographic information, and progress to encryption of recorded strings of data, to preclude counterfeiting and tampering efforts.

The ADIT document provides INS enforcement activities with a valuable identification tool in itself. The automated identification system currently being implemented will greatly enhance the security and utility of the identification system.

The ADIT System has evolved in response to changes made by INS management. These changes were the result of exhaustive studies of the Service's needs, priorities for allocation of resources, as well as lessons learned in the employment of the system. For instance, a major decision was made to defer deployment of machine card readers at ports of entry until closer coordination in the use of machine-readable technology could be effected between INS and other government agencies. INS, the Department of State, and the U.S. Customs Service have been engaged in a continuing dialogue regarding machine-readable passports and identification cards, and the use of equipment for verifying these entry documents, and the effect of such utilization on the twin goals of enforcement and facilitation. In the meantime, primary reliance for computer verification of the cards has been shifted to the use of video computer terminals. Our studies indicate that joint use of video terminals for inquiries to the the ADIT system, the lookout data base, and for adjudication purposes is most cost-effective.

Presently, there are 96 INS locations which have direct access via computer terminal to the ADIT card data base. Another 55 will be installed in FY 1984. These terminals provide INS officers at field locations with the capability to positively compare identity data to the information contained in the INS data base. Additionally, INS officers have and are utilizing the capability to call a base station from patrol vehicles and obtain relayed information from the computer data base. This information, coupled with the many security features incorporated in the

physical construction of the card, provides INS with the capability to intercept altered or counterfeit cards, and to detect imposters who attempt to use lost or stolen cards. More importantly, it provides a positive system for verifying the identify of lawful card holders.

The I-94 INS Arrival-Departure Record for nonimmigrants has recently received attention for its vulnerability to fraud. Meetings have been held with an I-94 interagency working group in an attempt to resolve problems resulting from other agencies' acceptance of the I-94 as an identity document. In addition to INS staff, the meetings were attended by representatives from the Departments of Housing and Urban Development, Labor, Agriculture, and Health and Human Services, the Social Security Administration, the Office of Refugee Resettlement, and Food and Nutrition Service.

As INS has stated in the past, the Form I-94 is intended for recording the admission and departure of aliens to and from the United States. Information recorded on this form is entered into an automated system to provide accurate and timely information on individuals and groups of nonimmigrants. However, it is clear that in many cases, the I-94 is currently being accepted as an identification document. It is used for the issuance of drivers licenses, for assigning Social Security numbers to some individuals, such as refugees, and is often the only means for determining eligibility for certain benefits including food stamps, rent subsidies and others.

INS is approaching this issue on two fronts: to educate benefit granting programs of the limitations of the Form I-94 as a sole identification document, and to provide a quality form of documentation to those aliens entitled to benefits. With respect to the first factor, INS has corresponded with the departments and agencies represented at the I-94 working group meetings to reiterate that the I-94 has been developed by INS for statistical purposes and alien registration only. We indicated our willingness to respond to inquiries as to whether such a document is

recorded in our system associated with the named individual. The information was also sent to the Departments of Motor Vehicles in each state, with an expressed belief that inter-agency efforts are required to identify a practical and reliable way of addressing the identification requirements needed by various agencies. Responses have been received from several state and federal agencies; and, I am confident that educating these agencies in the shortcomings of the I-94 as an identifier will help reduce fraud and abuse.

INS is presently issuing quality identification documents to Haitians being released under the court order in Louis vs. Nelson. This document, which is modeled after the ADIT card, will improve control of aliens in this class, by utilizing forensic features built into the document design in conjunction with an automated data base on card holders. Expansion of this program to document other groups of aliens admitted or paroled into the United States, who are entitled to certain benefits, is contemplated, consistent with the availability of resources.

Another common INS identification document used by aliens temporarily in the United States is the Crewman's Landing Permit, Form I-95A. This form contains the alien's name and date of birth as personal identifiers.

Two other documents, previously issued by the Service and still extant and valid, are the I-185, Nonresident Alien Canadian Border Crossing Card, and the I-186, Nonresident Alien Mexican Border Crossing Card, the latter of which has been replaced by the ADIT Form I-586. Both cards contain the alien's name, date of birth, address, and photograph.

Other identification documents issued by the Service include citizenship and naturalization certificates, which are issued to United States citizens who have acquired such status derivatively or through judicial naturalization. These documents incorporate personal identifiers of name, date of birth, and photograph. Administrative data include the former alien registration number of the individual, a certificate number, and date and court of naturalization.

The Form I-197, Citizenship Identification Card, which the Service no longer issues, is still extant and valid as an identifier of United States citizens.

CONTROLS ON THE ISSUANCE OF DOCUMENTS

Both legal and administrative requirements apply to the abuse or the misuse of the identification issuance system. Administrative controls consist of security clearances for employees; established standards and operating procedures for applicant processing, card production, and issuance; physical security measures at the card facility, and surveillance by the Office of Professional Responsibility to prevent abuse of the system by INS employees.

Application for the ADIT I-551, Alien Registration Receipt Card, begins at a Department of State consular office for new immigrants, or at an INS Files Control Office in the U.S. for aliens adjusting to immigrant status. Either a foreign service or INS officer is responsible for adjudicating the application, and positively identifying the applicant. Adjudicated applications are then forwarded, in accordance with control procedures, to the card facility. Cards are fabricated and the associated data base records created within a secure facility, operating in accordance with established standards and procedures, and manned by security-cleared personnel.

Form I-586, Nonresident Alien Border Crossing Cards and the Haitian ID cards are issued under similar control conditions, except that the Department of State has no involvement.

As has been noted, the Form I-94 Arrival-Departure Record was not intended to be an identity document, and no controls for security of the document itself exist. However, an INS officer does follow established procedures in issuing these sequentially numbered documents and controlling their

authorized use. An automated data base, the Non-Immigrant Information System, is accessible to provide information on the individuals to whom the I-94's were issued.

The I-95A, Crewman Landing Permit, is not issued to a large number of aliens and is not considered a valuable document for employment or resident purposes. Its issuance is controlled by an INS officer, who must ascertain the identity of the crewmember.

Certificates of Naturalization and Citizenship are issued as the result of an INS adjudication. That adjudication includes both review of the complete background file relating to that individual and a personal interview, where the identity of the applicant must be ascertained. Approximately 225,000 of these documents are issued annually.

Legal restrictions on the illicit production, use, and distribution of these documents are comprehended in federal counterfeiting statutes, principally Title 18 U.S.C. 1028, 18 U.S.C. 1426, 18 U.S.C. 1543, and, 18 U.S.C. 1546. Ancillary statutes include Title 18 U.S.C. 911, 18 U.S.C 1001, 18 U.S.C. 1015, 18 U.S.C. 1423, 18 U.S.C. 1424, 18 U.S.C. 1425, 18 U.S.C. 1427, 18 U.S.C. 1542, and 18 U.S.C. 1544. Title 18 U.S.C. 1028 gives the Service more direct jurisdiction in prosecuting document fraud and is proving invaluable to the Service's mission to thwart this type of fraud.

PERSONAL IDENTIFICATION INFORMATION SHARING

Personal identification information is supplied to the Federal Bureau of Investigation, Central Intelligence Agency, Department of Labor, Department of Agriculture, Department of Education, Deparment of Housing and Urban Development, Department of State, and the Department of Health and Human Services. Information is supplied to state and local agencies on a case by case basis. Dissemination of the identity and status information is handled by the Associate Commissioner, Examinations. The

Associate Commissioner, Enforcement controls release of information with regard to investigative matters. The Associate Commissioner, Information Systems is responsible for the system and procedures for information interchange.

Most of the release of information to date has been accomplished by individual case requests to INS, or by the matching of groups of individuals via automated "off-line" batch processing. For the individual case, INS may perform an on-line terminal inquiry to automated files, a manual search of paper files, or both.

As the volume and completeness of our automated files grow, so does the volume of requests for individual identity and status data from other federal and state agencies. This currently is prompting a serious look at allowing other agencies remote terminal access to our data bases. Certainly efficiencies could be gained by INS and the inquiring agencies. However, a number of factors must be considered and resolved prior to wholesale committal to this approach. First, are the technical aspects, such as data and telecommunication system linkages and transaction loads. Second, are all the associated costs and how to prorate such. Third, and probably most serious, are the privacy and freedom of information implications. Technical solutions are currently being developed in response to each of these three factors.

Most cumbersome is the privacy and freedom of information area. Present requirements call for either the individual to sign a consent statement prior to disclosure of personal information, or a notice of intent to disclose information be made publicly and a record of accountability for each disclosure maintained, available to that individual under freedom of information stipulations. Differing circumstances will require the employment of both methods. This is an added overhead to processing, filing, file storage and file retrieval.

Principal INS files to be accessed by other agencies are the Master Index System (MIS) and the Nonimmigrant Information System (NIIS). Both contain basic identity data, i.e., name, date of birth, status codes, and file location within the MIS, and name, date of birth, status codes, and local address within the NIIS. Inquiries support both service to the alien and enforcement needs.

On the front side of INS processing are interactions with the Department of State. Presently, immigrants and refugees arrive at ports of entry with their documents in hand. The alien is inspected and, if admitted, his documents are used to establish the official paper and automated file pertaining to him. A system goal for 1984 is to test the automated transmission of alien identity data, from point of initial processing by the Department of State or by INS (usually a consulate or refugee processing center), to central INS data bases. This action can collectively contribute to accuracy, standardization, and security of data, as well as protect against fraud. HHS and eventually other agencies will be included in this network, to identify uniformly an alien, and document the individual's activities throughout the time of interest to the U.S. Government, i.e., until naturalization, death, or emigration.

All physical and electronic access to INS data files is controlled by established procedures. Entry to file rooms and terminal locations is restricted. Terminal access to remote data bases is controlled via use of system passwords. Replacement systems to be implemented in FY 1984 will, based on terminal and user identity, control access to specific data bases, records and data elements.

IDENTIFICATION DOCUMENTATION PROBLEM

INS is concerned with document use and fraud in two major areas: (1) documents to gain entry into the United States and, (2) use within the United States by persons here illegally, as well as legally, to obtain benefits to which they are not entitled. At our international ports of

entry, many foreign nationals attempt to enter the United States through impersonation of a legal document holder or with altered or counterfeit documents. Within the United States, similar fraud is perpetuated to support claims to legal residence, and to gain benefits from federal, state, and local governments.

Our investigative experiences have clearly demonstrated to us that there is extensive counterfeiting, trafficking, and criminal use of personal identification documents to illicitly secure employment, illegally effect entry to the United States, or obtain benefits and services such as welfare, unemployment compensation, and federally insured grants and loans. This is true not only of those documents evidencing nationality or indicating legal permanent resident status, but also of those types of non-federal governmental identification which may be used independently or to generate such documents.

BREEDER DOCUMENTS

With one key identification document, which we might call a "breeder", an individual can secure or derive other local, state, or federal identification documents with relative ease. Breeder documents may be counterfeit, altered, fraudulently-secured, or imposter-presented. Common breeder documents include birth certificates, voter's registration cards, driver's licenses, foreign documents such as passports with U.S. visas or notations indicating U.S. residence, Social Security cards, immigration documents such as the I-151 or I-551 ADIT card or an I-94 Arrival-Departure Record for an alien classification which authorizes employment , and U.S. passports.

With a counterfeit or fraudulently procured state birth certificate, for example, an alien can secure a U.S. passport, Social Security card, driver's license, and voter registration card. The birth certificate also can be used by the alien to fraudulently enter the United States when arriving directly from Western Hemisphere countries, or can be used to petition for alien relatives to enter the United States.

Birth certificate frauds are particularly insidious because the individual posing as a U.S. citizen frequently evades the very systems designed to screen aliens for eligibility for benefit programs. For this reason, state birth certificates are highly prized by illegal aliens. The birth certificates may be counterfeit, obtained by schemes such as fraudulent registration by midwives, or secured by imposters who assume the identity of a native born citizen who may be living or deceased.

The magnitude of this one problem alone may be gauged by the fact that the El Paso Intelligence Center (EPIC) annually receives data on the use of approximately 12,000 birth fraudulent documents, the majority of which are counterfeit or imposter-presented Texas birth records. Some of the individual records and documents have been used by up to fifty different aliens, in locations as widespread as California and Illinois, and more than one hundred documents have been used by five or more individuals.

Aliens frequently rely on more than one fraudulent document to establish their false claims to United States citizenship, their eligibility for employment,or their entitlement for benefits. Aliens are thus induced to acquire genuine documents through the use of the initially procured fraudulent document. The more paper bred by the original document, the more deeply entrenched in the community becomes the violator. Or so he feels. Time constraints, inaccessible data bases, or the belief that the other agency has already verified the documentation passing through its system, can work against one agency confirming that the documents allegedly issued by another are genuine.

EXTENT OF PROBLEM

We have found that there is a huge potential market for bogus documents because of a large illegal alien population. As with illicitly sold controlled substances, the street price of a document often indicates its availability and ease of fabrication. While some document packages are sold for as much as $10,000, combination Social Security card and alien

registration card packages have sold in the past six months on the streets of Chicago for as little as $35.

In the nine month period of October 1982 through June 1983, our enforcement officers reported 12,372 violations of Title 18, U.S.C. 911, false claim to United States citizenship; 688 violations of Title 18, U.S.C 1426, counterfeiting or use of fraudulent naturalization or alien registration documents; and, 63 violations of Title 18, U.S.C. 1028, fraud and production of false identification documents. Twenty-four of these 63 violations of Title 18, U.S.C. 1028 were accepted for prosecution, and 14 convictions obtained prior to June 30, 1983. Fifty-six of the violations were reported in the third quarter, an eight-fold increase over the number reported during the first quarter the statute was in force.

DOCUMENT FRAUD TASK FORCES: INS DOCUMENTS AS BREEDERS

INS investigators have extensive experience in the investigation and prosecution of the users and producers of fraudulent documentation, and are attacking the vast problem of fraudulent documentation on several fronts. As the counterfeiting of Service identification documents strikes closest to home, INS is concentrating its investigative efforts on identifying and prosecuting those individuals who counterfeit and sell, or facilitate the fraudulent acquisition of bogus INS forms. Document Fraud Task Forces have been organized in both the Chicago and Los Angeles areas, for example, to specifically target the vendors of counterfeit alien registration cards and other Service documents. As Social Security cards, birth certificates, Selective Service registration cards, and voter's registration cards are also commonly obtainable through these same dealers, other agencies frequently participate with our officers in these task forces. Working undercover and using consensual monitoring, our investigators have successfully arrested and prosecuted over twenty-five major document vendors and counterfeiters in these two areas alone in the past nine months. Search warrants executed in conjunction with these arrests have netted nearly 19,000 counterfeit alien registration receipt cards, some of which were of the most recent issue (ADIT Form I-551),

nearly 8,200 counterfeit Social Security cards, numerous counterfeit California and Illinois birth certificates and driver's licenses, illicitly procured Cook County voter's registration cards, over $8,000 in counterfeit U.S. $10.00 bills, a number of illegally possessed firearms, and a small quantity of drugs. One illegal alien arrested in Huntington Park, California as a document vendor was in possession of 18,000 counterfeit alien registration cards and 7,500 counterfeit Social Security cards alone. This particular alien was prosecuted and convicted under Title 18, U.S.C. 1028.

Similar successful investigations and prosecutions have been conducted this year in Del Rio, Detroit, Newark, Dallas, New York City, Hartford, Seattle, San Francisco, Miami, Reno, Harlingen, El Paso, Houston, San Juan, Denver, Tucson and Boise. When these cases have involved the counterfeiting, sale, or procurement of Social Security cards by fraud, and have been coordinated with agents of the Department of Health and Human Services, they come under the aegis of a joint investigative effort called "Project Baltimore". Over one hundred and twenty individuals have been convicted nationwide in "Project Baltimore" cases since 1978.

VOTER REGISTRATION FRAUD

State and local governments and individual officials, who make it easier for constituents to obtain certain non-federal documents, may unwittingly or deliberately play into the hands of illegal aliens seeking documentation to which they are not entitled as a major investigation of the voter registration procedures in Chicago, Illinois has demonstrated. At the request of Dan K. Webb, the United States Attorney for the Northern District of Illinois, twenty INS officers collaborated with nearly two hundred officers from other federal and state agencies to monitor the elections held in Chicago in November, 1982 and February, 1983, and investigate allegations of voting fraud. Investigations conducted prior to the elections disclosed that over 1250 non-citizens had registered as voters in the City of Chicago. We found that it was much easier to obtain

a voter's registration card, which required no identification, than to obtain a county library card, which required two separate pieces of identification.

As Mr. Webb testified before the United States Senate Judiciary Subcommittee on the Constitution on September 19, 1983:

> We have found that many illegal aliens register to vote for the purposes of acquiring voter registration cards, which they then use to commit additional crimes. We have found instances of illegal aliens using an illegally obtained voter registration card to fraudulently obtain passports, public aid, and food stamps. We also found that on one occasion a non-citizen used an illegally obtained voter registration card in order to get security clearance to work for a contractor selling weapons parts to the United States Department of Defense.
>
> Furthermore, our investigation shows that some of these aliens actually cast illegal votes in various elections. We have found instances in which some persons have actively sought the registration of illegal aliens for the very purpose of influencing the outcome of an election....
>
> The illegal alien registration problem stems in part from the ease with which persons may register to vote in Illinois. Persons who want to register to vote should be requested to furnish identification....

Convictions have been obtained in the cases of seven aliens charged with offenses related to their illegal registration and voting, including passport fraud and fraud against the government. INS and the Office of

the United States Attorney have referred to the State's Attorney's Office twenty-nine additional cases resulting in indictments on state charges. The aliens involved in these schemes were nationals of Mexico, Belize, Costa Rica, Nicaragua, Haiti, Colombia, and the Philippines.

PROJECT SHEPHERD: NON-SERVICE DOCUMENTS AS BREEDERS

INS investigators are focusing efforts on uprooting vendors providing breeder documents to illegal aliens who use the documents to obtain welfare, to enter the United States by posing as United States citizens, or to acquire immigrant visas for relatives by fraudulently establishing citizenship, kinship, or gainful employment. We coincidentally found that many of these same vendors are fabricating other documents which are used simply to make life easier. We uncovered a corrupt state employee who was selling genuine New York State driver's licenses and vehicle registrations to unqualified individuals, and vendors who sold counterfeit high school, college, and university degrees to individuals who lacked the educational prerequisites for certain occupations. We even discovered one entrepreneur who provided counterfeit city marshals' eviction notices to individuals who posed as marshals, and "cleaned out" the apartments of neighbors who had been arrested by city authorities or immigration officers.

Since July 1981, INS investigators at New York City working on this massive umbrella case, dubbed "Project Shepherd", have identified thirty-two separate criminal conspiracies to produce and sell fraudulent documents to illegal aliens from Caribbean countries. Over one thousand counterfeit Puerto Rican birth certificates, one thousand counterfeit Puerto Rican certificates of identity, one thousand counterfeit Social Security cards, five hundred genuine driver's licenses and vehicle registrations which had been issued by a bribed New York State employee, and several thousand counterfeit bank letters, tax returns, and miscellaneous INS forms have been seized in connection with these cases. Thus far, twenty counterfeiters and fraudulent document vendors have been

convicted for their parts in the conspiracies. Those who were convicted are United States citizens, legal permanent resident aliens, and illegal aliens. Some were receiving welfare, while others were employed as travel agents, immigration consultants, printers, and auxiliary New York City police officers. As a further result of the disclosure of massive fraud, one U. S. consulate in the Caribbean denied fifty-two percent of its pending immigrant visa applications.

NON-SERVICE BENEFIT FRAUD

The Service's enforcement efforts are also being channeled to meet the formidable threat posed by aliens who circumvent the Immigration and Naturalization Service to gain benefits other than those which the Service grants or has under its jurisdiction. These benefits include entitlements at the federal, state, and local levels, and involve programs such as welfare, food stamps, unemployment insurance, subsidized housing, student loans, and state dividends (e.g., Alaska Permanent Fund Dividend Program). The Service actively pursues attempts to fraudulently obtain these benefits on two fronts: the criminal and administrative.

First, the Service exchanges identifying data with other government agencies at all three levels to insure that neither benefits nor identifying documentation is provided to ineligible aliens or groups of ineligible aliens.

A computer-matching program has been established with the Department of Housing and Urban Development, for example, to insure that illegal alien applicants do not receive housing subsidies. Certain individuals who blatantly have received such subsidies are pursued criminally. In New York City last October, twenty West African nationals who had obtained over $100,000 in housing subsidies in the South Bronx were arrested by INS and HUD investigators, and seven prosecuted for false statements concerning income and family composition.

Information exchange programs have also been established with the Department of Labor Unemployment Insurance Service, the Social Security Administration, and the Department of Education. In the three month period of June through August 1983, information sharing programs at all levels nationwide identified 4,378 ineligible alien applicants for entitlements such as unemployment insurance, Social Security benefits, public assistance, and guaranteed student loans, and netted a potential savings to various governments of over $23,000,000. Many if not most of the ineligible aliens had made false claims to legal permanent resident status through the use of counterfeit alien registration receipt cards or false claims to United States citizenship through the use of counterfeit California birth certificates.

In California , under a project called the "CA-6 Program", which has been in operation since 1976, the immigration status of all alien applicants for Social Security and welfare benefits are verified against Service records. This program alone generated a potential savings to the State of California of $20,000,000 in the three-month period cited.

Liaison with the Department of Education in conjunction with the Student Loan Investigation Program has resulted in the identification of 490 ineligible aliens and a savings of $2,640,500 to the U.S. government. A number of the aliens who obtained loans through false statements have been prosecuted and deported.

SOLUTIONS TO FRAUD PROBLEMS

INS has, of course, recognized an ever increasing level of fraudulent identification document activity since the 1940's, when Alien Registration Receipt Card issuance began. We have taken several measures, over the years, to both increase the quality and security of our identification systems and to improve our capabilities for detecting and countering document fraud.

The Service is responding to the problem of alien use of fraudulent identification by concentrating its enforcement efforts on investigating and prosecuting those who counterfeit, sell, or arrange for others to acquire such documentation. To support this, INS totally restructured its internal control over investigative cases this July to place its greatest emphasis on pursuing violators of this genre.

First, consider the increased sophistication of fraud. The capability to fabricate bogus documents has increased and detection has become more difficult. INS has waged a continuing battle to remain ahead of the counterfeiters in technical capabilities and knowledge. Our Forensic Document Laboratory (FDL), which was established in 1979, provides scientific analysis of questioned documents and subsequent expert testimony in resultant criminal cases. The FDL conducts research in the field of document fraud, provides technical assistance to field personnel, and assists in efforts to develop counterfeit-proof identification documents. Much of the work done by the Forensic Document Laboratory in the area of foreign passport and non-immigrant visa issuance is coordinated with appropriate offices of the Department of State.

Further steps must be made to heighten the awareness of all agencies to the problem of the use of fraudulent identification lest one agency's efforts to counter fraud are to be translated into another agency's increase in fraud. Whatever efforts are needed should be taken to encourage states to institute programs to match death records with birth records, or limit access to "dead infant records". California, for example, recently initiated a program to match the death and birth records of infants.

We have in the last four months gone out at the local district office and sector levels to state agencies which issue identification documents such as birth certificates, state identification cards, and driver's licenses to alert them to a potentially large increase in fraudulent activities by aliens spurred by the prospect of massive immigration reform legislation.

Currently we are accumulating samples of state issued documentation from these same sources in order to build a reference resource of both forensic and operational value in our efforts to screen counterfeit forms.

The Service is working with government entities at all levels to share records and intelligence for the purpose of denying entitlements to ineligible aliens, locating regulatory weaknesses for the purposes of sealing system loopholes, and identifying arrangers who abet violations for the purpose of stopping their activities. In the past two years, INS has initiated meetings with other agencies to begin or to expand areas of information sharing or data base exchange. In line with the Service's new investigations case management system, increased priority has been given to such cooperative efforts to staunch the flow of benefits or documents to those not entitled to them.

Additional memoranda of agreement between agencies still need to be formulated or expanded to increase computer-matching. Privacy concerns about information release and the requirement of providing written notification to each individual about whom data is released, have, however, become serious administrative obstacles to implementing such programs especially considering the high costs involved.

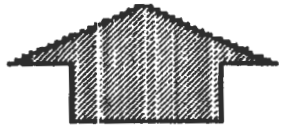
Another area of grave concern centers on the negative impact the Tax Reform Act of 1976 has had on information sharing with the Social Security Administration. SSA cannot generally provide to INS data which has been fed into its systems by the Internal Revenue Service. These provisions of the Tax Reform Act are in direct conflict with the information sharing provisions of Section 290(c) of the Immigration and Nationality Act (Title 8, U.S.C. 1401), and have effectively served to thwart Social Security Administration efforts to cooperate in locating illegal aliens. This critical problem should be addressed through corrective legislation.

Thank you for the opportunity to provide testimony to the committee. INS shares your concerns and belief that the identity document questions and problems are one of the most important issues facing the nation today.

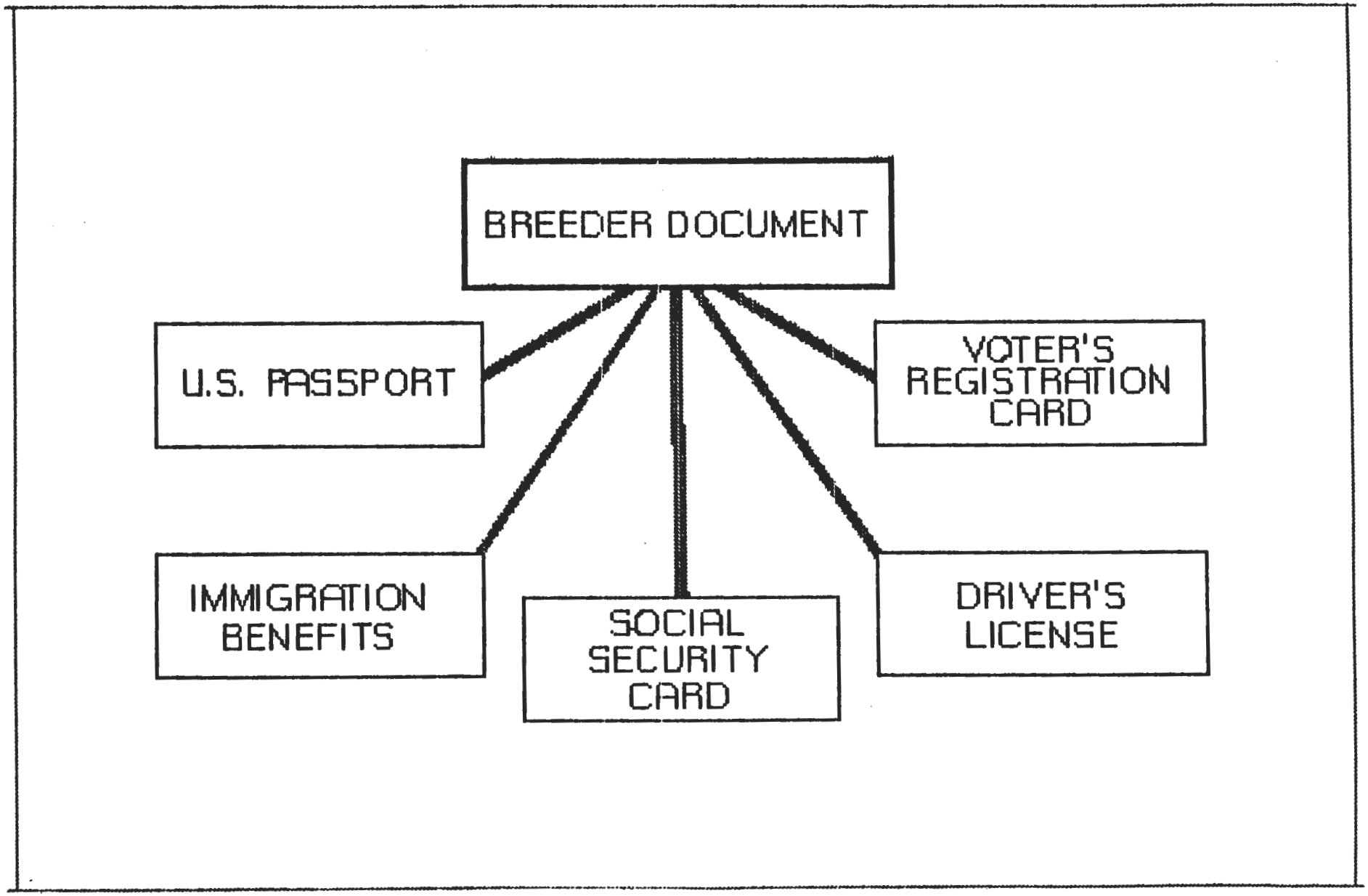
BREEDER DOCUMENTS

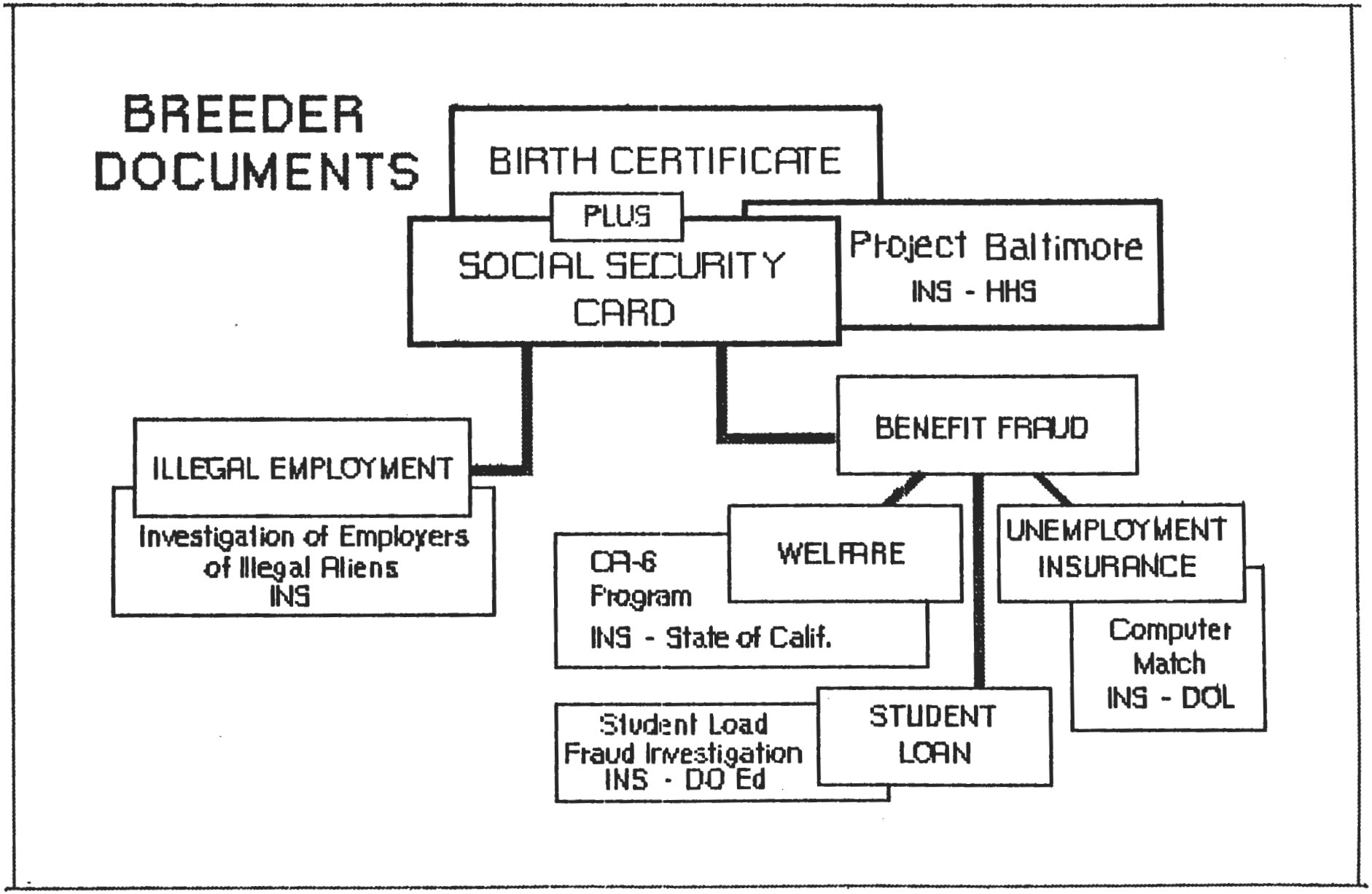
- BIRTH CERTIFICATES
- IMMIGRATION DOCUMENTS
- U. S. PASSPORTS
- FOREIGN DOCUMENTS
- SOCIAL SECURITY CARDS
- VOTER'S REGISTRATION CARDS
- DRIVER'S LICENSES

BREEDER DOCUMENTS



- COUNTERFEIT
- ALTERED
- OBTAINED THROUGH FRAUD
- IMPOSTER - PRESENTED


BREEDER DOCUMENT
U.S. PASSPORT
VOTER'S REGISTRATION CARD
IMMIGRATION BENEFITS
SOCIAL SECURITY CARD
DRIVER'S LICENSE


BREEDER DOCUMENTS
BIRTH CERTIFICATE
PLUS
SOCIAL SECURITY CARD
Project Baltimore
INS - HHS
ILLEGAL EMPLOYMENT
Investigation of Employers of Illegal Aliens
INS
BENEFIT FRAUD
WELFARE
CA-6 Program
INS - State of Calif.
UNEMPLOYMENT INSURANCE
Computer Match
INS - DOL
STUDENT LOAN
Student Load Fraud Investigation
INS - DO Ed

BREEDER DOCUMENTS

SOLUTIONS:

- HEIGHTENED AWARENESS OF FRAUD
- LIAISION AND INTELLIGENCE
- ENHANCED FORENSIC CAPABILITIES
- COMPUTER MATCHING
- LEGISLATIVE AND REGULATORY INITIATIVES