E·C·I
ECONOMIC CRIME INSTITUTE

LexisNexis®

Identity Fraud: A Critical National and Global Threat

A Joint Project of the Economic Crime Institute of Utica College and
LexisNexis, a Division of Reed Elsevier Inc.

October 28, 2003

Dr. Gary R. Gordon
Professor of Economic Crime Programs
Executive Director of the Economic Crime Institute
Utica College

Mr. Norman A. Willox, Jr.
Chief Officer for Privacy, Industry, and Regulatory Affairs
LexisNexis, a Division of Reed Elsevier Inc.

Foreword

In its continued effort to provide cutting edge research, the Economic Crime Institute has partnered with LexisNexis to conduct this research study on Identity Fraud. LexisNexis provided the funding for the study. This study is a continuation of two earlier works on identity fraud sponsored by LexisNexis. Norman Willox, Jr. and Thomas Regan authored "Identity Fraud: Providing a Solution" in March 2002. It can be retrieved at http://www.lexisnexis.com/about/whitepaper/IdentityFraud.pdf. An earlier work by Willox and Regan entitled "Identity Fraud: Searching for a Solution," was released in October 2001. The URL is: http://www.lexisnexis.com/risksolutions/IdentityFraud.pdf.

About the Authors

Dr. Gary R. Gordon is the principal author of this study. He is Professor of Economic Crime Programs at Utica College and the Executive Director of the Economic Crime Institute.

Mr. Norman A. Willox, Jr., Chief Officer for Privacy, Industry, and Regulatory Affairs, LexisNexis provided directional and expert support.

Mr. Thomas Regan, Esq., is Executive Director, Privacy and Regulatory Affairs, for LexisNexis. Mr. Regan was the main contributor to Section IV and provided insightful comments throughout the document.

Two individuals from Utica College provided additional support: Dr. Donald Rebovich and Ms. Judy Gordon, M.L.S. Dr. Rebovich, associate professor of Economic Crime Programs, was the main contributor to section II. Ms. Gordon's contribution included extensive research, editing of the overall document, and writing in several sections.

Economic Crime Institute of Utica College (www.ecii.edu)

The Economic Crime Institute of Utica College supports education and research in economic crime and information security, providing a reliable resource for innovative solutions to corporate, government, and law enforcement entities. It provides the Economic Crime Investigation and Management faculty of Utica College with support for the development of academic programs and provides a national forum for the exchange of ideas on economic crime and fraud management. The Institute's dynamic leadership and innovative ideas are drawn from its Directors, forward thinking executives who are experts in the prevention, detection, and investigation of economic crime and fraud.

LexisNexis

In the US, LexisNexis (www.lexisnexis.com), an information solution provider, offers an extensive range of products and customized tools that address job-specific and organization-wide information needs, driving productivity and confident decision-making. LexisNexis draws on its 30-year history of data expertise to develop leading applications, which assist customers in authenticating identity, mitigating risk, predicting fraud, and acquiring more customers. With LexisNexis, customers may see measurable results such as increasing customer acquisition, reducing identity fraud, reducing fraud losses, predicting fraud, and streamlining investigation processes. LexisNexis focuses in the industries of financial services and collections, insurance, law enforcement, the federal government, retail, Internet transactions, and telecommunications. For more information on LexisNexis™ Risk Management, visit: http://www.lexisnexis.com/riskmanagement.

Table of Contents

Executive Summary

Identity Fraud: A Critical National and Global Threat

Identity fraud is a national and global threat to the security of nations and their citizens, the economy, and global commerce, as it facilitates a wide range of crimes and terrorism. While there have been numerous studies and reports on identity theft, this white paper discusses the differences between identity fraud and identity theft, as well as their similarities. The paper also considers legal, societal, and technical approaches to managing identity fraud while recognizing their policy and practical limitations. The key issues addressed in this paper include:

- Identity fraud, a quantitatively and qualitatively larger problem than identity theft, threatens national security, global commerce, and the protection of society.
- Advanced research, a national identity fraud classification system, and statistical assessments are required to evaluate and monitor the various permutations, root causes, and criminal implications of identity fraud.
- There is an indisputable need for identity authentication, especially information-based identity authentication, to manage the identity fraud problem. The known paucity of global data sharing must be addressed.
- Fundamental privacy interests must be balanced with the need for personal information in identity authentication applications.
- Information sharing policies and technical solutions are crucial to managing identity fraud while enhancing privacy protection.
- A national and global strategy is essential in order to combat identity fraud.

The Identity Fraud Threat

Identity theft has been at the forefront as a societal problem for several years. The public has been made aware of the dangers of identity theft, particularly to personal and financial security. Many studies have been completed concerning the size and scope of victimization. The government, credit card and other financial service industries have responded by putting tighter controls in place. On the other hand, the insidious threat of identity fraud has not been similarly acknowledged. Both the public and private sectors must understand and confront the enormity of the identity fraud problem so that it can be solved. Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime. It often emanates from a breeder document created from fictitious or stolen identifiers. The breeder document, such as a driver's license or birth certificate, is used to spawn other documents, resulting in the creation of a credible identity which allows a criminal or terrorist access to credit cards, employment, bank accounts, secure facilities, computer systems, and the like. Once a criminal or terrorist has an established identity, he can use it to facilitate a variety of economic crimes, drug trafficking, terrorism, and other crimes.

At one time, not that many years ago, a breeder document, such as a driver's license, meant something; it could be used to establish a person's identity with little or no question. Now, technology has enabled criminals to produce fraudulent documents, which can be used to procure additional fraudulent documents. Counterfeit documents, such as credit cards, used to be easily detectable; now it is relatively easy to produce a counterfeit hologram that usually passes for the real thing. Counterfeit documents are now readily available to illegal immigrants, drug traffickers, and international terrorists. Technology and the ability of the criminal element to adapt and defeat existing identification methodologies, predicated on breeder documents that are susceptible to counterfeiting, have made it necessary to develop different, more advanced identity authentication systems.

Identity fraud is a component of almost every major crime and its presence is felt throughout the world. Therefore, it is absolutely essential that the importance of identity authentication is recognized whenever the potential result of misidentification is the commission or perpetuation of criminal activity. Government and industry leadership is necessary to facilitate the development of policies and technological tools that will assure accurate identity authentication.

Advanced Research and National Identity Fraud Classification

Identity fraud has become the enabling agent, in effect, the catalyst, for various types of financial crimes, terrorism, drug trafficking, and other crimes. In the case of the 9/11 terrorist attacks, several of the terrorists are alleged to have used fraudulent identification documents such as driver's licenses, stolen credit cards, fictitious and/or temporary addresses, false passports and other fraudulent travel documents, and fictitious Social Security Numbers. Although the terrorists' commission of identity fraud is one of the most notorious cases, there are many others. However, there is no system in place for collecting statistical data on identity fraud, so that its size, scope, and impact can be understood and addressed. Most of the available statistics concentrate on identity theft and its victims, rather than identity fraud.

The implementation of a research agenda, including a national system for identity fraud classification and collection of data on identity fraud is crucial. Analysis of the data will expose trends and criminal behavioral patterns which will provide the basis for the development of prevention and detection methods and the promulgation of legislation and regulations.

Need for Information-Based Authentication and Global Data

The only system of authentication that focuses on determining the validity of personal identifiers is information-based identity authentication, a form of knowledge-based authentication. When a person is new to an institution and there is no trusted credential or biometric, the only reliable means to determine that the person is who he says he is, is an information-based identity authentication system. An information-based system of identity authentication is an independent assessment of what the individual in question represents about his identity, based on an analysis of available information pertaining to that individual. It applies three levels of risk management: validation, verification, and authentication. To be effective, such a system must incorporate the following critical components: risk, cost, speed of decision making, availability of information, and the sophistication of the individuals/organizations making the threat. Generally speaking, as the risk or threat increases, more sophisticated methods of risk management must be employed. The system must address an increased risk or threat by continuously evaluating additional types and quality of data from domestic and global sources. Additional data needs may result in increased operational cost, the need for more sophisticated delivery systems, and further refinement of global and domestic information sharing policies.

The paucity of global data, a widely acknowledged problem, hampers the effectiveness of an information-based identity authentication system and, therefore, must be addressed. The 9/11 terrorists attacks highlight the deficiency of global information and point out how imperative it is to acquire and integrate such data in order to authenticate identity.

Balancing Privacy Interests with the Need for Personal Information

An information-based identity authentication system is dependent on personally identifiable information, which is information that is identifiable to a real person. The collection, use, and distribution of such data has privacy implications. The extent of the privacy implications is sometimes defined by law, but even in the absence of applicable legal principles, it is shaped by notions of fair use. However, fair use of personally identifiable information is a relative notion requiring context for application.

Privacy interests in the information used for identity authentication must be balanced with the particular need for identity authentication. This requires an assessment of the potential harm that misidentification in a given transaction might cause. For example, if the risk of harm from misidentification in a transaction is a terrorist event, then the use of sensitive personally identifiable information might be justified. However, even in such a context, fair information use considerations apply, as the data used must be proportional. That is, the data used in the identity authentication process must be relevant and necessary to accomplish the requisite confidence level of authentication. Also, fair information practices, such as notice, choice, access, security, limited use, and enforcement, should be employed in the identity authentication process to the extent practicable.

Information Sharing Policies and Use of Technology

To effectively combat identity fraud, authentication solutions must respond to the continuously changing face of the criminal. As the criminal surmises the process for identity authentication, he will eventually attempt to craft an identity to avoid the detection system. This process of detection avoidance must be matched through constant monitoring of the effectiveness of the identity authentication system, continuous upgrading of data sets, regular enhancements in the algorithmic models, and other technological changes.

The need for continuous changes in the sources, types, and quality of data require the existence of a trusted environment. This trust must envelop the relationships among data owners, data aggregators, data users, and data subjects. To create this trusted environment, information sharing policies, in the form of rules, must be established that govern how data can be used, the persons who can access it, and the purposes for its use. Most importantly, adherence to the rules must be verifiable within the context of appropriate oversight; the more sensitive the information, as seen through the eyes of the data owner or subject, the greater the need for verification to occur in real or near real time. Technological tools to accomplish this requirement are available and should be deployed.

A National and Global Strategy to Combat Identity Fraud

Legislation and regulations, information policies, technological solutions, education and training, and public awareness have attempted to combat identity fraud. However, because those efforts have not yet been enough, implementing a national and global strategy is crucial. The many challenges to doing so are raised throughout the white paper and include: easy access to false identifiers, limitations on domestic and global information sharing, privacy and information security policy, domestic and global policy, dedicated resources, and leadership.

In the United States, the federal legislation that has been developed to address the identity fraud problem has focused on two means of risk mitigation: first, the criminalization of conduct relating to identity fraud; and second, the strengthening of tools designed to authenticate the identities of individuals. The solutions offered have focused on the criminalization of the misuse of identities and the imposition of tighter privacy and security requirements on the use of personally identifiable information. Even when particular legislation has promoted identity authentication, it has been biometric and credential-based, while, with limited exceptions such as Section 326 of the USA PATRIOT ACT, failing to recognize the need for information-based identity authentication solutions.

This study recommends several courses of action including a national and global identity authentication strategy based on improved data collection, focused research, information sharing policies, and technology applications to facilitate sharing while insuring privacy. Seven core recommendations are presented:

1. **Gain a commitment from the highest levels of federal government to lead and fund a national strategy to combat the identity fraud problem.** Strong national leadership and significant resources are required to combat this growing domestic and global problem.

2. **Establish a central information database of identity fraud incidents.** There is a great need to measure the size, scope, and trends of identity fraud. This can only be done through a new national identity fraud classification system.

3. **Establish a national identity fraud research agenda.** Several research studies are proposed to increase the knowledge of identity fraud in terms of the size and scope of identity fraud, how criminal organizations use identify fraud as a facilitator of their crimes, the effectiveness of identity fraud investigations and prosecutions, and the characteristics of victims.

4. **Establish more sophisticated domestic and global information-sharing networks.** The key to identity authentication is access to data to assist in the validation, verification, and authentication of personal identifiers. While some information-sharing networks do exist, they are fragmented, limited, and not easily accessible. Greater access is required, especially for global data, to determine if the identity presented is valid.

5. **Study domestic and global policies, laws, and regulations to determine the best practices to combat identity fraud.** A comprehensive study of existing domestic and global laws and regulations concerning identity fraud, data collection, and information sharing will ascertain areas of ambiguity and gaps, review potential remedies, suggest methods of sharing data, and propose model identity fraud laws. These results should yield a best practices approach for managing identity fraud and be the first step in developing agreements for promulgating comprehensive laws and sharing data on a global basis.

6. **Develop a policy to enhance the protection of individual privacy and information ownership.** Inherent in all of the recommendations proposed in this white paper is the goal of enhancing the protection of privacy. As solutions are developed to combat identity fraud, it is crucial to consider the enhancement of individual privacy and information ownership. Policies which require the protection of privacy while balancing the need for information sharing must be established.

7. **Improve information sharing systems that enhance identity authentication solutions while protecting privacy.** Because the initial enrollment period is the critical stage in preventing identity fraud, an information based authentication system is the only solution that truly addresses the issue. While identity authentication systems currently exist, they are not robust enough nor do they provide the requisite privacy and information security that must be included in a trusted system. Therefore, the focus must be on the research and development of a trusted system that will effectively and efficiently authenticate identity, while maintaining the privacy and security of personal identifier information.

Identity fraud is a growing national and global crisis. Its pervasiveness must be recognized, especially as a facilitator of crimes that threaten national security, the economy, and global commerce. If identity fraud is not seen as a significant and insidious threat, it will not be dealt with accordingly. Without a national and global strategy, identity fraud will continue to grow exponentially, as will the possibility of financial crimes, terrorist acts, drug trafficking, gun running, and alien smuggling, all of which have an adverse impact on the global community and commerce.

♦♦♦

Part I
Introduction

Identity fraud has become a major concern for the public and private sectors, particularly as it relates to terrorism, money laundering and financial crime, drug trafficking, alien smuggling, and weapons smuggling. It is defined as the use of false identifiers, fraudulent documents, or a stolen identity (identity theft) in the commission of a crime, and has been used for decades by criminals and criminal organizations to help facilitate their criminal activities and to avoid detection. Identity fraud is broader than identity theft in that identity fraud refers to the fraudulent use of any identity, real or fictitious, while identity theft is limited to the theft of a real person's identity.

However, it was the events of September 11, and the investigation conducted afterwards, that awakened society to the fact that the criminal use of false identifiers and false identification documents is not just a significant component of fraud, but also of terrorism. Further examination has revealed that the criminal use of false identifiers and false documents is an integral part of many crimes committed by global criminal groups, including drug traffickers, gun runners, cyber criminals and alien smugglers. In each of these areas, the organized criminal enterprises exploit weak or non-existent verification systems. This broad criminal use of false identifiers and false identification documents requires a new term, a term different from "identity theft, " which has a more limited connotation. In this White Paper, it is referred to as "identity fraud."

While identity theft has long been recognized as a crime that pervades our society, identity fraud has not. There are many websites that provide the public with tips to avoid having their identities stolen and remedies to employ if they are victims of identity theft. As evidenced by the passage of identity theft laws and other regulations since 1998, there has been a dramatic increase in the widespread use of these methods by criminals and terrorists. This has been facilitated by the exponential growth of the Internet, allowing illegal access to personal identifiers through hacking and to websites that demonstrate how to create and/or obtain fraudulent documents. Awareness of identity fraud has also grown. "The events of September 11, 2001, have heightened concerns about the contributory role that identity fraud plays in facilitating terrorism and other serious crimes." (Stana, June 25, 2002) However, there is no single data source that compiles and reports all incidences of identity fraud, making the measurement of the size and scope of the problem very difficult. Because identity fraud is used to facilitate crimes, information about it is not reported separately, but as a part of many other types of crime. There is no central repository for data that is collected and none of the federal government repositories, such as the UCR (Uniform Crime Reports) and NIBRS (National Incident-Based Reporting System), collect specific data on identity fraud or theft. Most of the available information comes from industry organizations or individual federal government agencies such as the Federal Trade Commission. Limited conclusions about identity fraud and theft can be gleaned from the statistics that are gathered by such agencies.

The credit card industry began collecting data on identity theft and account takeovers in the mid 90's. Although identity theft accounted for a very small percentage of total credit card fraud, various industries and legislators were forced to respond to it sooner than otherwise would have been the case because of the insidious way in which it destroys individuals' credit ratings and impacts their financial stability. "In fiscal year 1995, the Postal Inspection Service began tracking mail theft cases involving fraudulent credit-card applications and change of addresses. In October 1997, also in reference to fraudulent credit-card activity, the Secret Service began tracking cases involving identity takeover" (Identity Fraud, May 1998). The Identity Theft and Assumption Deterrence Act of 1998 made it illegal to, "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." The act also focused on the consumer as a victim and set up a central repository for reporting the crime. "In November 1999, the FTC established the Identity Theft Data Clearinghouse to provide a central repository of consumer complaints about identity theft" (Federal Trade Commission, August 30, 2000). Drawing on statistics from many of these sources, this paper provides an extensive assessment of the growing problem of identity theft and fraud.

As the size and scope of the problem begin to be understood, it is evident that identity fraud is linked to many global crimes, including terrorism, money laundering and financial crimes, drug trafficking, alien smuggling, and weapons smuggling. The horrific events of September 11, 2001 and the resulting focus on terrorism have brought much scrutiny and attention to identity fraud as far more than a crime against consumers. Security concerns have quickly emerged in the areas of immigration, border crossings, airline passengers, Hazmat (hazardous materials) driver's licenses, and pilot training. At the center of all of these concerns is the need to authenticate individuals to determine if they are who they claim to be.

With little in place to stop identity fraud or to adapt as the perpetrators change their methods, seeking the highest return for the lowest risk, both domestic and international perpetrators are able to establish legitimate identities for themselves. Once they have stolen an identity and/or created a false identification document, they are able to create a fraudulent identity for themselves which allows them to cross borders and then provides them access to such identification documents as birth certificates, drivers' licenses, and social security cards. Those documents, in turn, create greater access by allowing them to procure employment, credit cards, green cards, bank accounts, marriage certificates, leases, mortgages, and the like. With a job, a permanent address, and a credit record, they have established a credible identity. That credible identity enables them to engage in criminal activity – financial crimes, money laundering, smuggling, etc. – for profit, concealment, and/or to support terrorism.

Identity fraud will continue to grow exponentially until there are systems in place to authenticate individuals. New laws and regulations, technology, education, training, strong leadership, and information policy are needed to control identity fraud. Without access to specialized data bases and trusted technology, and the education and training necessary to operate them, decision makers are ill equipped to make accurate assessments in very short periods of time. Laws and regulations are necessary in order to insure that policies and methods of determining identity are uniformly applied and so that criminals can be held accountable for their wrongdoings. Information policy will provide direction for information sharing and the resolution of privacy issues. There are many challenges to developing the means to stop this growing problem, including global policy, limited data analysis and the inability to measure the size and scope of the problem, sharing of public and private information, issues surrounding protection of privacy, the availability of and easy access to false identification sources, and dedicated resources for development and implementation of technology, education, and training. A strong line of defense is essential to prevent skilled criminals and terrorist from gaining access to entry points that allow them to commit crimes of profit and terrorism.

To that end, an analysis of legislative and regulatory efforts with respect to identity theft and fraud, the continuing risks and vulnerabilities, and an assessment of additional legislative and regulatory efforts needed to address those risks and vulnerabilities are presented here. Also addressed are fraudulent conduct, privacy, information sharing, and appropriate access, distribution, and use policies.

An analysis of current laws and regulations is not enough, however. Authentication methods and proven risk management strategies that provide the basis for faster and more effective decision making must be developed and employed in determining identity. Information analysis, including scoring and modeling, enable this model. Information sharing and data integration from three key sources, commercial, private, and public, provide the fodder for performing sophisticated information analysis, which can then be shared across the affected parties. This analysis must occur within a trusted environment.

Model systems, such as Radiant Trust, provide examples of potential solutions for sharing appropriate information in order to facilitate identity authentication. The challenges this serious societal problem poses are many; the authors attempt to answer those challenges by providing recommendations to manage them.

♦♦♦

Part II
Size and Scope of the Identity Fraud Problem

Identity Theft[1]

Determining the frequency and growth of any crime area is a daunting task. Official statistics generated from data gathered by law enforcement entities (e.g., the FBI's Uniform Crime Reports) afford some degree of insight into key characteristics of the crimes, but account for only those crimes that are reported to authorities. Such statistics are also directly affected by shifts in enforcement strategy that could influence reporting patterns. Victim surveys partially solve the problem of uncovering the "dark number" of unreported crimes, but often suffer from non-response bias and are dependent on the victim's memory and complete understanding of the victimization. These and other common problems inherent in measuring criminal activity are amplified when an attempt is made to determine the extent of identity theft in the U.S.

The relatively newly evolved crime category of identity fraud presents additional problems for measurement accuracy. Identity theft is frequently not counted by law enforcement agencies as a discrete crime, but as a subset of other economic crimes; this can unintentionally mask the frequency and gravity of identity theft when criminal occurrences are tabulated. Another problem is that the collection of raw data on identity theft is decentralized and largely dependent on an amalgam of federal, state and local enforcement data that, in some respects, is piecemeal and in other ways is duplicative. Finally, because identity fraudsters are able to sustain their criminal activities for extended periods prior to victim awareness of the crimes, the aforementioned victim survey drawbacks for collecting valid data are exacerbated. In short, achieving a true measure of identity theft in the U.S. today is one of the most challenging tasks facing the law enforcement community.

The most noteworthy attempt to synthesize the extent of identity theft has been conducted by the U.S. General Accounting Office (GAO). The GAO reports on identity theft furnish a glimpse of identity theft patterns in the U.S. For its report titled, "Identity Theft: Prevalence and Cost Appear to be Growing," (General Accounting Office, March 1, 2002, GAO-02-363) the GAO relied upon multiple sources for its measurement of identity theft. The GAO combined original interview data from law enforcement officials with documentation from represented law enforcement agencies (i.e., the Federal Bureau of Investigation [FBI]; Internal Revenue Service [IRS]; the Social Security Administration [SSA]; Secret Service; Postal Inspection Service; and the Federal Trade Commission [FTC]). The GAO merged this information with data collected from three national consumer reporting agencies and two payment card associations (MasterCard and VISA).

Victim data, reported by individual victims of identity theft to the FTC, was generated primarily through GAO's Identity Theft Data Clearinghouse. From November 1999 through September 2001, the Center reported a consistently rising total of identity theft. The GAO points out that the FTC averaged 445 identity theft reports per week in November 1999. The total rose to over 2,000 reports per week in March 2001 and over 3,000 reports per week in December 2001 (General Accounting Office, March 1, 2002, GAO-02-363)

In a more recent study, "Federal Trade Commission—Identity Theft Survey Report," released September 3, 2003, the results of a victimization survey, conducted during March and April 2003, of a randomly selected group of over 4000 participants in the United States are reported. The study's objectives included "estimate the incidence of identity theft victimization" and "measure the impact of identity theft on the victims (p. 2)." The study classifies identity theft into three categories: "new accounts and other frauds, misuse of existing non-credit or account number, and misuse of existing credit card or credit card number (p. 4)." The results indicate that 4.6% of those surveyed had been victims of at least one of the forms of identity theft in the past year. When generalized to the U.S. population, the extrapolated figure of identity theft victims in the US in the past year is 9.91 million. The reported losses to business including financial institutions for all forms of identity theft were estimated at $47.6 billion. This figure was derived by multiplying the average loss per victim in each of the three categories by the number of victims in each category. Using the same methodology described above, the cost to victims was assessed. The out of pocket expenses to rectify the identity theft victimization was estimated to be $5.0 Billion (p. 7). Respondents were

[1] For the purposes of this section, the term "identity theft" is used more frequently than "identity fraud," because agencies which report these crimes use the category "identity theft."

also asked about victimization in the past five years. The results indicate that within the last five years, 27 million adults in the United States have been victims (p. 12).

This study provides the most credible estimates of the size, scope, and financial impact of identity theft victimization in the United States to date. Unfortunately, the study sheds little light on the identity fraud problem. The report indicates, "3% of victims said that they were aware that the thief had used their personal information to obtain government documents, such as a driver's license or social security card (p. 37)." The authors suggest that this number may be low because victims would only know this information if they were informed by law enforcement or other government organizations.

In his testimony before the U.S. Senate Judiciary Committee's Subcommittee on Technology, Terrorism and Government Information of the Senate Judiciary, Howard Beales, director of the FTC's Bureau of Consumer Protection, provided a characteristic breakdown of the FTC Identity Theft Clearinghouse report data (*Identity Theft: the FTC's Response*, March 12, 2002). At that time, Mr. Beales reported that in terms of geographic location, the state of California ranked first in number of identity theft victimizations, followed by New York, Texas, Florida, and Illinois. For victimizations per capita (i.e., per 100,000 citizens), the District of Columbia was first, followed by California, Nevada, Maryland and New York. When analyzing the report data by victim's age, it was found that those in younger age groups were more likely to be victims of identity theft. Victims in their thirties were most susceptible to victimization, followed by those between 18 and 29. Those in their forties comprised the third leading group (see Table II-1). The reports involved a variety of ways in which the stolen identity was used, including credit card fraud and unauthorized telecommunications or utility services (see Table II-2). One of the telling statements of Mr. Beales' testimony was that an average of twelve months elapsed between the commission of the crime and the victim's discovery of it.

Table II-1
FTC Identity Theft Clearinghouse
Report Data – Age

Age of Victim	Percentage
Under 18	2
18-29	26
30-39	28
40-49	22
50-59	13
60 and over	9

Table II-2
FTC Identity Theft Clearinghouse
Report Data – Uses of Stolen Identity

Crimes Where ID Used	Percentage
Credit card fraud	42
Unauthorized telecommunications or utility services	20
Bank fraud	13
Personal information for employment purposes	9
Fraudulent loans	7
Procurement of government documents or benefits	6
Other identity theft	19
Used for multiple crimes	20

Updates of FTC data from the FTC's Consumer Sentinel and the Identity Theft Clearinghouse for calendar year 2002 have demonstrated that key identity theft characteristics have remained constant except for volume. Percentage distributions by age of identity theft victims were nearly identical to that in 2001, reflecting a victimization pattern somewhat younger than the typical fraud victim. Accounting for 43% of the total fraud complaints for 2002, identity theft topped the FTC's list of consumer frauds for the third year in a row. (As a percentage of all consumer fraud complaints, identity theft has risen from 22% in 2000 to 39% in 2001 to 43% in 2002). The District of Columbia again was home to the highest rate of identity theft complaints followed, once more, by California but with Arizona replacing Nevada as third highest rate in the nation. The most notable difference from 2001 was total volume of identity theft complaints; from 86,198 in 2001 to 161,819 (Federal Trade Commission, January 22, 2003).

The Social Security Administration's (SSA) Office of the Inspector General (OIG) also houses a fraud "call-in" reporting center. The OIG uses allegations of Social Security Number misuse as an indicator of identity theft. The OIG reports a dramatic rise in these allegations, from approximately 11,000 in fiscal year 1998 to 62,376 allegations in fiscal year 1999. The 1999 figure rose to

83,721 in fiscal year 2000 and to 104,103 in fiscal year 2001 (General Accounting Office, June 2002, GAO-02-766). According to the OIG, over 80% of the Social Security Number misuses are forms of identity theft. The FTC arrived at this percentage by collecting a statistically representative sample of 400 allegations from October 1997 through March 1999 and documenting which of the allegations were considered crimes of identity theft (General Accounting Office, March 1, 2002).

The GAO also sought out another more creative manner of gauging the extent of identity theft by turning to the number of 7-year fraud alerts placed on consumer credit files. These data were generated by three consumer reporting agencies. The fraud alerts serve as warnings of potential fraudulent use of an individual's personal information to obtain credit, and advise the credit grantors to take further steps to verify the identification of the person attempting to use the credit card. The reporting period of the generated data partially overlaps with that of the FTC, but was not the same for all three agencies, thus diminishing the ability to make across-agency comparisons. Nevertheless, the data reported by the two agencies demonstrates an increase of identity 7-year fraud alerts over time (see Table II-3).

Table II-3
7-Year Fraud Alerts

Consumer Reporting Agency	1999	2000	Increase
1	65,600	89,000	36%
2	19,347	29,593	53%

Thus the first consumer reporting agency reported a 36% rise in the alerts and the second reflected a 53% increase. A third consumer reporting agency reported their number of fraud alerts as 92,000 for the year 2000, but was unable to supply data for a base year for comparison purposes (General Accounting Office, March 1, 2002).

Aggregate data from MasterCard and Visa on monetary loss as a result of identity theft focused on two indicators of identity theft: account takeovers and fraudulent applications. The GAO reported that the combined domestic identity theft losses suffered by the two associations rose 43%, from $79.9 million in 1996 to $114.3 million in 2000. Complementing this cost data, the American Banking Association (ABA) reported to the GAO that identity theft accounted for 56% of all check fraud for community banks (i.e., those banks with assets under $500 million) and 29% of all banks in the U.S. (General Accounting Office, March 1, 2002, GAO-02-363).

Other data collected on identity theft were largely anecdotal, with some estimates coming from Los Angeles, the city ranked by the FTC Clearinghouse as the third largest city for identity theft victimization reports (General Accounting Office, June, 2002). As of May 2001, the Los Angeles County Sheriff's Office reported 2,000 active cases and the Los Angeles Police Department reported 5,000 cases of identity theft. Updated information from the Los Angeles Police Department in March 2002 revealed that identity theft cases had risen to an estimated 8,000, 70% of which involved utility or cellular telephone fraud. The remaining 30% involved credit card fraud and check fraud. (General Accounting Office, June, 2002).

Because federal law enforcement agencies in the U.S. do not specifically track identity theft cases, the GAO depends on certain proxies in an attempt to estimate the extent of identity theft growth. The most popular of these proxies is "identity theft-related crimes." For example, the GAO reports that the FBI's arrests for bank fraud rose from 579 in 1998 to 691 in 1999 and then declined to 645 in 2000. The Secret Service reported that they had 8,498 identity theft-related cases closed in 1998. That number dropped to 7,071 cases closed in 2000, possibly because of the agency's policy shift to a focus on "high-dollar" loss cases. The amount of fraud losses in these cases averaged $73,000 for 1998 and $218,000 in 2000 (Stana, June 25, 2002).

The GAO also reported that identity theft cases in which the offender fraudulently used identifying information of a fictitious person was becoming pervasive within alien groups. As reported to the GAO by the Immigration and Naturalization Service (INS), the use of fraudulent identification documents rose from fiscal year 1998 through fiscal year 2000 and dropped in fiscal year 2001 (1998 – 99,171; 1999 – 120,715; 2000 – 123,537; 2001 – 114,023). Approximately half of the fraudulent identification documents intercepted by the INS were border crossing cards and alien registration cards (Stana, June 25, 2002)

The information presented above represents the best aggregate data on identity theft available at this time. While the information gleaned through GAO research provides identity theft characteristics, patterns, and volume, caution should be exercised in the interpretation of the results. Data on various indicators of identity theft are currently being collected by several government agencies. However, they are working independently and are using disparate definitions of identity theft and methods of gathering data on these crimes. Therefore, it is difficult to draw conclusions about the extent of identity theft and fraud. Is identity theft rising? Based on all known indicators, it is rising annually. However, there is a clear need for a centralized agency responsible for collecting standardized national data on identity fraud. This is the only way we will be able to measure the size and scope of this major societal problem.

Identity Fraud and Criminal Activity

The use of a false identity created from fraudulent documents or a stolen identity (identity theft) in the commission of a crime has long been used by criminals and criminal organizations to facilitate criminal activities and avoid detection. As is evident from the previous section, quantifying the impact of identity fraud is difficult, but as the statistics in the next sections report, terrorism, money laundering and financial crimes, drug trafficking, alien smuggling, and weapons smuggling are growing concerns for the public and private sectors. Laws and regulations that have been instituted since 1998 are another indicator of the dramatic increase in the widespread use of these methods by criminals and terrorists.

Terrorism

While the fight against terrorism has been longstanding in the U.S. and abroad, it is not surprising that the emphasis on terrorism and its control has grown dramatically since the September 11, 2001 terrorist attacks on the U.S. An army of law enforcement agencies from national and local government have embarked upon the challenging task of identifying terrorists and terrorist-related activities through coordinated investigations and, in turn, bringing terrorists to justice through successful criminal prosecutions. As we enter the initial phase of the post 9/11 war on terrorism, obvious questions arise regarding the size and scope of terrorism, both domestic and international, and what amount of progress enforcement agencies are realizing in their efforts. Past parameters of terrorist-related activities are being constantly reset to adapt to their evolving criminal endeavors.

It is clear that the scope of criminal activities extends beyond the core terrorist acts to financial crimes committed to support terrorist operations. In Senate hearings, the Federal Bureau of Investigation has underscored the threat posed by identity fraud and Social Security fraud engaged in by terrorists in order to obtain employment, access to secure locations, driver's licenses and bank/credit card accounts, all for the purpose of financing their criminal activity. The FBI's Terrorist Financial Review Group has accelerated its aggressive pursuit of terrorist groups by collaborating with the Social Security Administration in the investigation of SSNs identified through past terrorism investigations and by widening the traditional scope of terrorist investigations. Such investigations now include the targeting of fraud schemes committed by loosely organized groups who use the proceeds to fund terrorist groups (Lormel, July 9, 2002).

As with attempts to gauge the extent of other crime areas, an understanding of the breadth of terrorism relies upon statistics of enforcement actions. For several reasons, including definitional, exact numbers of terrorist/terrorist related arrests, prosecutions and convictions have been hard to discern. However, research conducted through the Transactional Records Access Clearinghouse (TRAC) at Syracuse University paints a revealing portrait of terrorist enforcement conducted through the U.S. Department of Justice, and of its successes and deficiencies.

TRAC analysis of DOJ referrals for criminal prosecution for suspects of international terrorism revealed that such referrals ranged between 57 and 83 referrals per month for the study period of 09/01-3/02. Referrals for domestic terrorism initially peaked in October of 2001. By March, 2002 there were 118 referrals. (See Table II-4.) The referrals themselves were fairly evenly spread throughout the nation, accounting for 87 federal districts. At least 10 terrorism suspects were referred for prosecution from 28 districts, representing every region of the U.S. The top international terrorist case referrals were clustered around Washington DC (Virginia East – 47; Maryland – 36; and the District of Columbia – 33), California East (Sacramento – 28), Iowa North (Cedar Rapids – 22), and Michigan East (Detroit – 20). The top regions for domestic terrorism referrals were North Carolina West (Asheville – 68), Virginia East (Alexandria – 29), and Tennessee Middle (Nashville – 22).

Table II-4
TRAC Analysis of DOJ Referrals

	9/01	10/01	11/01	12/01	1/02	2/02	3/02
International Terrorism	85	77	57	57	83	76	71
Domestic Terrorism	45	90	79	41	39	46	118

Monthly numbers of prosecutions and convictions for terrorism lag behind the rise in referrals for the September 2001-March 2002 period. At the time of the TRAC report, federal prosecutors had acted upon one third (328 out of the total 945 referrals for domestic and international terrorism). At the time of the report 185 cases had been disposed of, with only 20 of them ending in conviction. Median sentences on terrorist case referrals for this period were 3 months for domestic terrorist cases and 5 months for international terrorist cases. These represent cases that have made their way relatively quickly through the criminal justice system, such as immigration, ID and visa violations (TRAC, June 17, 2002).

Despite the fact that the Department of Justice's Executive Office for U.S. Attorneys' definition of terrorism emphasizes actions furthering political goals through force or threat of force, many criminal charges for the six month study period did not involve such acts. Thirty-three different lead charges were reported in connection with international terrorism cases. The most common charges involved terrorism of an unspecified nature or supplying support to terrorism, but were frequently declined by prosecutors. Cases with lead charges of fraud and misuse of identifying documents, visas and passports were the next largest group, most of which were taken to court by prosecutors rather than declined. These types of cases also comprised the largest group – approximately one-third of the total of domestic terrorism cases referred.

The most dramatic change for types of terrorism cases can be seen when comparing the composition of charges filed for the six-month study period with the previous five years. The most common charges for international terrorism from the beginning of 1997 through September 11, 2001 were kidnapping, murder, and hostage taking. The most common charges for domestic terrorism cases during this period were the importation and storage of explosives. The most common terrorism charges from September 12, 2001 through March 2002 involved fraud. From 9/12/01 through 3/02, in 39.9% of the combined international and domestic terrorism cases, the lead violations were general *fraud/false statements* (18 USC 1001). Such charges made up only 4.8% of the federal charges for terrorism (combined international and domestic) for the preceding five year period. Other fraud categories that evidenced a less dramatic rise in lead charges (from the preceding five year period) were fraud and related activity – ID documents (18 USC 1028) - .9% to 4.4%, and fraud and misuse of visa permits (18 USC 1546) – 4.3% to 6%. (Note: Caution should be used in the emphasis of this rise since it could be the result of isolated cases with multiple defendants and since the raw numbers are so low. Much of this increase could be attributed to the March 2002 case involving 66 Hispanic workers at the Charlotte/Douglas Airport. These figures more likely represent a shift in enforcement strategy [flexible categorization of what constitutes terrorism] than an increase in fraud committed by terrorists).

Money Laundering

Money laundering is a crime problem area that has historically been associated with drug traffickers' efforts to introduce the proceeds garnered through the sale and distribution of illegal drugs into the legitimate financial market. The U. S. Drug Enforcement Agency (DEA) estimates that funds laundered for these illegal purposes exceed $600 billion per year (DEA, 2003). Other estimates for the total worldwide amount of money laundered range between $600 billion and $1.8 trillion. This represents between 2% and 5% of the world's gross domestic product. Federal law enforcement has been active in attempting to control money laundering. The number of defendants sentenced in cases with money laundering as the primary sentencing guideline rose steadily between fiscal years 1996 and 2001 (see Table II-5).

Table II-5
Defendants Sentenced in Federal Money Laundering Cases

Fiscal Year	Number
1996	843
1997	932
1998	973
1999	1066
2000	1106

(U.S. Department of Treasury, July 2002)

While drug trafficking remains a primary driving force for money laundering, the combination of financial services globalization and technological advances has made money laundering a growing threat to financial institutions. One indicator of this is the pattern of Suspicious Activity Reviews (SARs) filed by financial institutions in the U.S. Between April 1, 1996 and November 1, 2002, the top category of SARs filed was BSA/Structuring/Money Laundering (491,988) accounting for 48.2 % of SARs filed during that period (Bank Secrecy Act Advisory Group, February, 2003; TSA, 2003).

A report by Transaction Systems Architects (TSA) provides insight into recent high profile cases emblematic of money laundering's threat to financial institutions and the diminishing public confidence in financial institutions suffering from ineffective money laundering detection programs and/or employee complicity with money laundering operations. These high-profile cases were reported by TSA as follows.

Bank of New York Victimization – Starting in February 1999 and ending in August 1999, a former vice president of the Bank of New York and her husband created Bank of New York accounts for three companies and facilitated 160,000 unauthorized wire transfers for Russian bank customers totaling over $7 billion. As a result of this case, the Bank of New York entered into an agreement with the U.S. Federal Reserve requiring the development of an effective money laundering control program to prevent future occurrences of this type.

Operation Casablanca – This was a 1998 U.S. Customs Service money laundering sting that resulted in the conviction of 28 bankers from two of Mexico's largest banks. Part of the money laundering operation involved 13 wire transfers made by the head of the Miami office of Banco Industrial de Venezuela totaling $4.1 million.

Noncompliance Cases – These cases involve banks falling out of compliance with government regulations to combat money laundering. Between April 1999 and April 2000, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCen) imposed penalties on nine banks for noncompliance with the Bank Secrecy Act (BSA) requirements totaling more than $1.3 million. Among the nine was Sunflower Bank, N.A. of Salina, Kansas, which had improperly filed 1,900 Currency Transaction Reports (CTRs).

While aggregate data on the use of identity theft and fraud in money laundering is not available, it is not too large a leap of faith to assume that the perpetrators did not always use their true identity – having either stolen one or procured and/or produced fraudulent documents to facilitate the money laundering and financial crime process.

Drug Trafficking, Alien Smuggling, Weapons Smuggling

These crimes are all facilitated by identity fraud. Once again, statistics compiled in these areas do not include identity fraud and/or theft as a separate category. However, it is clear from several cases that the use of identity fraud makes smuggling much easier. As Rand Beers, Assistant Secretary for International Narcotics and Law Enforcement Affairs, stated in his testimony before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information, "Both groups [smugglers and terrorists] bring corrupt officials whose services provide mutual benefits, such as greater access to fraudulent documents, including passports and customs papers…Both groups make use of fraudulent documents, including passports and other identification and customs documents to smuggle goods and weapons."

Drug trafficking is cited by agencies such as the Office of National Drug Control Policy (ONDCP) and the U.S. Customs Service as a crime problem that is growing without abatement. ONDCP estimates that the annual cocaine flow through the Transit Zone (encompassing the Gulf of Mexico, Caribbean Sea and the eastern Pacific Ocean, is more than 500 metric tons annually, 80% of which is smuggled by non-commercial maritime conveyances. ONDCP reports that the proportion of these conveyances that are "go-fast" boats (i.e., small, high speed smuggling boats invisible to radar) has increased substantially since 1995. Smugglers hold the competitive edge over interdiction vessels, resulting in an estimated 90% smuggling success rate for go-fast deliveries (ONDCP, January, 2002).

It is difficult to determine the amount of narcotics actually smuggled into the U.S. each year. However, amounts seized by the U.S. Coast Guard and the Customs Service provide an indication of the enormity of problem. In fiscal year 2001, the U.S. Coast Guard reported a record year for drug seizures; 138,393 pounds of cocaine and 34,520 pounds of marijuana.

Individual narcotics smuggling enforcement operations have underscored the gravity of the drug smuggling problem. In 2000, Operation Journey, a multinational enforcement effort conducted by the Drug Enforcement Administration (DEA), the U.S. Customs Service, and the Joint Interagency Task Force East ended a Colombian drug trafficking operation. The operation used commercial vessels to smuggle vast amounts of cocaine into 12 countries, primarily in North America and Europe. Over 16 tons of cocaine were seized by authorities.

In its report to Congress in May 2000, the GAO detailed the growing threat of alien smuggling. This threat primarily emanates from two types of smuggling organizations: "blue collar" smugglers and "white collar" smugglers. The blue collar smugglers consist of large numbers of Mexican nationals operating along the southwest border. White collar smugglers charge higher fees for their services, operate out of countries other than Mexico, and have more of an international scope. Alien smuggling conducted by both groups is on the rise. The International Organization for Migration estimates that approximately 4 million of the 100 million migrants worldwide have either been smuggled or trafficked (GAO, May 2000; Finckenauer & Schrock, 2000).

The GAO has reported that the number of apprehended aliens smuggled into the U.S. rose almost 80% between the fiscal years of 1997 and 1999. Data compiled by the Immigration and Naturalization Service (INS) revealed that the number of illegal aliens apprehended attempting to enter the U.S. increased from about 138,000 in 1997 to 247,000 in 1999. Fourteen percent of the 1.6 million illegal aliens apprehended by the Border Patrol in fiscal year 1999 were found to have been smuggled compared to 9% (of 1.4 million) in fiscal year 1997. The GAO has also cited the rising number and proportion of illegal aliens apprehended from countries other than Mexico as a sign of the increasingly serious nature of alien smuggling (These aliens are said to be more reliant on organized smugglers). Such aliens apprehended rose from 58,000 in fiscal year 1997 to 81,000 in fiscal year 1999 (GAO, May 2000).

Central America has been recognized as an important source and transit point for illegal immigration. According to INS' El Paso Intelligence Center (EPIC), Central American countries are home to 10 of the top 11 individuals smuggling aliens across the southwest border. It is unclear how many alien smuggling operations exist, but it is estimated that there are up to 300 such organizations in Mexico and up to 50 in Toronto, Canada. (Estimates are that the Toronto organizations transport 5,000 aliens into the U.S. each year). The INS views organized crime groups in Colombia, Nigeria, Albania and Russia as future sources of increasing alien smuggling. Special areas of concern are the smuggling of Russian prostitutes and People's Republic of China (PRC) nationals. The number of PRC nationals apprehended by the Coast Guard quadrupled from fiscal year 1997 to fiscal year 1999 – 240 to 1,100 apprehended (GAO, May 2000).

The INS sees the increasing use of fraud by alien smugglers as a critical problem. Alien smugglers are said to be using fraudulent documents to obtain immigration benefits (e.g., permanent residency and work authorization) for aliens smuggled into the United States. Smugglers have taken advantage of the Visa Waiver Pilot Program (VWPP) which allows nationals from some countries to enter the U.S. with only a valid passport. Smugglers have used both counterfeit and genuine passports from VWPP countries to smuggle non-VWPP nationals. (A common problem here has been PRC nationals at U.S. ports of entry using high-quality Japanese passports). Lost or stolen passports are particularly problematic because, being genuine, fraudulent use is hard to detect. The elimination of visa policies in other countries is also a facilitating factor for alien smuggling- related fraud. The INS estimated that in November of 1999, at least 100,000 VWPP passports were reported lost or stolen. The INS attributed the increase of the apprehension of Polish nationals (70 in fiscal year 1997, to 231 in fiscal year 1999) to the elimination of Mexico's visa policy for Poland (GAO, May, 2000).

The thorniest problem for INS is the fraudulent representation of U.S. employment for aliens. Alien smugglers have become active in creating fictitious companies for which the aliens would ostensibly work. Such fraud was discovered in over 90% of INS' analysis of 5,000 L-1 visa petitions, making it, as characterized by GAO interviews of INS senior managers, "the new wave in alien smuggling." (GAO, May 2000, page 12).

Effectively detecting the smuggling of weapons into the U.S. has become an especially elusive goal of the U.S. Customs Service due, in large part, to the increasing volume of people and conveyances crossing our borders. The U.S. Customs Services processed a total of 415 million pedestrians and passengers and 130 million conveyances in fiscal year 2002. (Processed conveyances include passenger vehicles, trucks, private and commercial aircraft, and small boats and vessels). Unable to inspect all but a small portion of entries into the U.S., Customs officials rely heavily on telltale smuggling signs and tips by informants to guide their enforcement efforts. In fiscal year 2002, U.S. Customs was able to focus such efforts on the serious problem of weapons smuggling and seize 39,643 firearms from weapons smugglers. However this is estimated to be only a fraction of the total number of firearms that pass under Customs' radar (U.S. Customs, 2003; Richey & Blair, June 3, 1998). Enforcement gaps were emphasized in a much-publicized experiment simulating nuclear smuggling conducted by the Natural Resources Defense Council and ABC News in which a 15-pound cylinder of depleted uranium was transferred undetected from the U.S. to Austria, Hungary, Romania, Bulgaria, Istanbul and back to the U.S. (Natural Resource Defense Council, September 11, 2002).

United States law enforcement officials have currently targeted the smuggling of military material from the U.S. to other countries as a grave threat to international security.

The new Bureau of Immigration and Customs Enforcement (the Department of Homeland Security successor to the former U.S. Customs Service criminal investigations office) has made the prevention of the illegal exportation of U.S. technologies and weapons systems to terrorist organizations and other U.S. adversaries a high priority (Solomon, March 4, 2003).

Recent cases illustrate how diverse the illegal exportation of U.S. technologies and weapons systems are both in terms of geographic destination and the types of material smuggled. One investigation in New York led to the disruption of a scheme to smuggle helicopter machine parts and military equipment through Switzerland to Iran. In December of 2002, an investigation in Connecticut foiled a plot to smuggle a military radar system into Bangladesh and another investigation in Milwaukee stopped three companies from exporting parts for F-4 and F-15 fighter jets and military helicopters into Iran. In February 2003, four individuals and three companies were indicted for attempting to export military equipment to China. Also in February 2003, Raytheon Corporation, the manufacturer of the Patriot missile, paid $25 million to the U.S. government for attempting to export sensitive communications equipment to Pakistan (Solomon, March 4, 2003)

The targeting of illegal exportation of U.S. technologies and weapons systems continues with the Bureau of Immigration and Customs Enforcement's "Shield America," in which heightened awareness has led to more than 5,700 U.S. companies and sellers of weapons technology being contacted. The new, enhanced enforcement strategy has widened the scope of focus beyond halting exports to banned countries, to include situations in which Americans permit themselves to be duped into selling sensitive military equipment without concern for the weapons' final destination (Solomon, March 4, 2003).

Conclusion

Identity fraud has become the enabling agent – in effect, the catalyst – for financial crimes, terrorism, money laundering, and drug trafficking, alien smuggling, and weapons smuggling. Our ability to address the problem is curtailed by the lack of any reliable, organized reporting system that accurately reflects all reported identity fraud, across agencies and jurisdictions, as well as international borders. While parts of the puzzle have been assembled from a variety of public agencies and private enterprises, the information is not comprehensive, nor is it shared through the use of a central database. Future studies, building on existing ones such as the September 2003 identity theft survey, will be needed to estimate the size and scope of identity fraud and its financial impact as a core facilitator of several types of crime. In addition, a reporting system and the ability to share it among all involved agencies and countries must be developed.

♦♦♦

Part III
The Role of Identity Fraud in Facilitating Criminal and Terrorist Activity

Identity fraud provides criminals and terrorists with the tools they need to remain anonymous, gain access, avoid detection, and transfer resources. There are many organized crime groups around the world perpetrating numerous violent and heinous crimes, most of which are supported by identity fraud. Several reports on organized crimes, such as Europol's report on organized crime in the European Union, the Library of Congress report on Asian organized crime in Canada, and the International Crime Threat Assessment, make note of the role of false documentation. "Terrorists and organized crime groups are also suspected of cooperating with each other to obtain forged documentation for identification and travel" (Library of Congress, 2003 July, p. 36). "Supportive crimes are also essential. The primary types of crime discussed above [drug trafficking, illegal immigration, human trafficking, commodity smuggling, etc.] cannot really be viewed in isolation from supportive activities such as document forgery" (Europol, 2002 October 3, p. 14). "Traffickers, however, also use fraudulent documents to obtain genuine travel documents or use altered or counterfeit documents to move the women and children" (International Crime Assessment, 2000 December, Chapter II, p. 11). Diagram III-1, the identity fraud process, depicts the overall process from the procurement of fraudulent or stolen identifiers to the end result of criminal or terrorist activity. Each phase is described below.

Phase I: Procure Fictitious or Stolen Identifiers

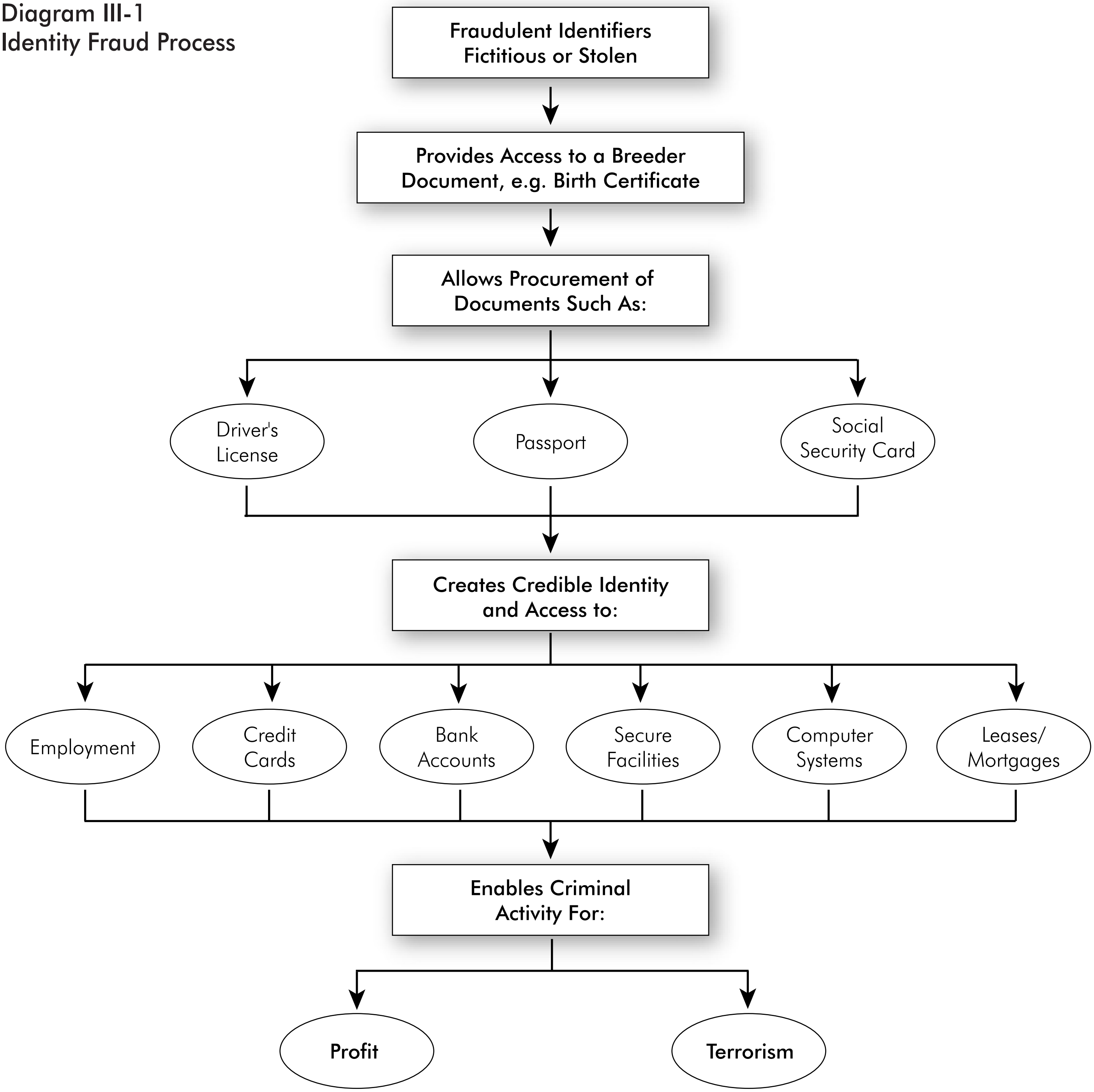
The identity fraud process begins with an individual creating a new identity, often using fraudulent identifiers or by assuming another person's identity (identity theft). Fraudulent identifiers allow the procurement of a fraudulent breeder document, such as a passport, birth certificate, driver's license, or a Social Security Number. Internet supported false documents or ones provided by a counterfeiter or forger open the doors to bona fide identifiers and breeder documents. A breeder document is a single fraudulently procured document, such as a driver's license, which provides the information necessary to procure additional fraudulent documents. Unlike documents obtained through the use of a stolen identity, there is no victim who may become aware of and report the theft, possibly leading to the apprehension of the criminal.

These documents are easily acquired by accessing various Internet sites, engaging corrupt officials, and/or accessing the counterfeit document underground. Detailed guides are available in how-to books and on the Internet for those who want to make their own false documents. Criminals use the Internet to distribute and sell fraudulent identifiers, fraudulent documents, and stolen identities. The Senate Permanent Subcommittee on Investigations completed a report, "Phony Identification and Credentials via the Internet," in February 2002. Their investigation found numerous websites that can provide false identification documents through several methods, including mail order purchase of such documents, purchase of a computer template for at-home production, and free computer software that can be used by any number of people any number of times to produce or create realistic, but false, identification. Their findings include:

> …many Internet sites offer a wide variety of phony identification documents, some of which are of very high quality and include security features commonly used by government agencies to deter counterfeiting. These include driver's licenses from all 50 States, birth certificates, Social Security cards, military identification cards, student identifications, diplomas, press credentials, and Federal agency credentials such as those used by the FBI and CIA. The Subcommittee also found products such as Social Security Number generators, bar code generators, and instructions for creating holograms….the Internet has played a leading role in fostering the manufacture and the sale of high quality false identification and has made these products available to a vast customer base with virtual anonymity for both the sellers and the buyers. This has, in turn, presented significant challenges for law enforcement. (Permanent Subcommittee, 2002, February, p. 2)

Europol found the same to be true. As stated in its *2002 EU Organised Crime Report, Public Version*, "There have also been significant developments in the area of computer and printer technology systems, increasing organised crime groups' capacity to produce counterfeit documentation of various types" (Europol, 2002 October 3, p. 8).

Diagram III-1
Identity Fraud Process



Procurement of Documents

Once a person has gained access to the country or procured fraudulent identifiers, he has the necessary identification to apply for fraudulent documents such as a driver's license. In the United States, a driver's license is used as the primary verification tool for establishing age and residency, and as the quintessential photo identification, e.g. for boarding a domestic flight. A United States passport, obtained with a stolen identity, and the identifiers for the stolen identity provide the needed information (i.e. date and place of birth) to apply for a "replacement" birth certificate or Social Security card.

Other fraudulent documents can be purchased on the "black market." The Immigration and Naturalization Service conducted an investigation in May 2002 in which "they arrested 24 persons and seized counterfeit documents and counterfeiting equipment May 8 in an operation designed to disrupt the continuing false document open-air markets in the Adams-Morgan neighborhood of Washington, D. C." Operation Card Shark, as it was called, netted "360 phony alien registration cards (green cards); 281 fraudulent social security cards; 70 bogus employment authorization cards; and 46 counterfeit drivers license from California, Utah, and Florida." (CommuniQUE, 5/02)

Access to Passports and other Border Documents

Border crossings are made easier by the use of false documents such as border crossing cards, nonimmigrant visas, passports, and citizenship papers. The quality of these documents is improving rapidly, making visual detection difficult. Organized crime groups use fraudulent documents to check-in aliens at overseas airports and to smuggle them into the countries such as the United States and Canada. Individuals with ties to terrorist groups have been found with fraudulent documents throughout the world. According to Paul J. Smith (July 1, 2001) notable cases in 1999 and 2000 involved a travel agency in India that provided fake passports for hijackers of an Indian airlines flight, an Arab man arrested in Kuwait for attempting to transport fraudulent Kuwaiti citizenship papers to Osama Bin Laden, and the founder of the Japanese Red Army who used forged passports as he traveled between Japan and China. Fraudulent documents can be obtained through stolen blanks, stolen and altered documents, counterfeiting, and by using fictitious information on applications., In April of this year, undercover federal agents proved that it is not difficult to gain entry to the Untied States with such documents.

> Undercover federal agents tested the nation's border security last month by trying to enter the United States with fake ID's after arriving on a one-way flight from Barbados. Offering bogus birth certificates, fake driver's licenses, and false names, they easily passed immigration inspection…Moreover, this was a re-test. The undercover agents from the U.S. General Accounting Office, the investigative arm of Congress, had used the same phony documents to win passage late last year at the Canada and Mexico borders. (COX NEWS, 2003, May 14)

The government is making efforts to increase the detection of fraudulent documents and to stop large criminal organizations involved in creating and distributing them. In his October 9, 2002 testimony to the Senate Judiciary Technology, Terrorism and Government Information Subcommittee, Michael Cronin, Assistant Commissioner for Inspection, Immigration and Naturalization Service, stated that the use of the State Department's Consolidated Consular Database resulted in

> detecting 108 fraudulent visa holders in the first six months [in Miami]. INS Inspectors using this data in New York caught an alien trying to enter the US on a falsified Russian diplomatic passport. In another instance, a 41-year old man was discovered using the altered visa of a three-year old Brazilian boy (Cronin, 2002 October 9).

In May 2002, the INS reported a six month investigation dubbed "Operation Big Man," in which the INS worked with other domestic and international law enforcement agencies in order to stop a large scale terrorist-related smuggling ring. They arrested several smugglers and document vendors.

> Besides the arrests, the investigators also seized numerous counterfeit or altered passports, four counterfeit Canadian visa foils, and two transparencies for making a counterfeit visa printing plate for U.S. visas…Another 19 "customers" were apprehended in connection with the bust. They were in the process of being supplied with false passports, visas, and other documents.(CommuniQUE, 2002 May)

Phase II: Create Credible Identity and Gain Access

Having a fraudulent identity provides criminals and terrorists with access to many other elements of a credible identity – personal identifying documents, bank accounts, government entitlements, and the like. As these accumulate, the criminals' authentic identity becomes more and more difficult to discern. Although they have been acquired with a bogus identity, they appear to be official documents. With a new identity, the criminals or terrorists can avoid detection by officials who are checking credentials, or fool systems used to detect fraudulent documentation. At each subsequent stage of the process, the individuals build a more credible identity as they collect more fraudulent documents and information is placed in a variety of databases. Ultimately, the criminals or terrorists have procured the documents necessary to provide them access to money, secure facilities, transportation, and whatever else is necessary for them to commit criminal or terrorist acts for profit or purpose. Several points of access are addressed here and access to others, such as computer systems, can be extrapolated from the discussion.

Access to Financial Institutions

Once the criminal has a driver's license, birth certificate, and/or Social Security card, he has established a substantive identity and is able to apply for credit cards, open bank accounts, and transfer funds. In a recent case in Queens, NY, 17 people were indicted in an alleged mortgage scheme.

> Queens District Attorney Richard Brown said the defendants are accused of "turning real estate closings into a game of Charades in which nothing was authentic except the money that changed hands." Prosecutors said the

> defendants would first pick a house, choosing six one-family homes in Queens, ranging in price from $200,000 to $250,000. They would then pose as a buyer and seller, creating false bank records, drivers' licenses and deeds, and set up a meeting with a mortgage company to obtain authorization for a loan… When the bank cut a check for the loan… defendants would divide the money between them. (Newsday.com, 5/9/03)

Clearly, fraudulent documents provide the necessary access to bank transactions. Bank personnel, especially tellers, are trained to examine identification, such as driver's licenses. If a driver's license is sufficient for proving identity, then there is no defense against fictitious documents.

Access to Federal Entitlement Programs
The U.S. Chief Financial Officer Council released a report in November 2002 entitled, "CFO-PCIE Improper and Erroneous Payments Work Group Sub-Work Group on Indicators Final Report on Indicators," which focuses on the techniques used to identify erroneous payments, indicators of erroneous payments, and limitations to the identification and prevention of such payments. One category of indicators is potential fraud. Listed in that category are "False claims, False or duplicate SSNs, False residence/ business address, Fictitious identity/non-existing business." Identity fraud is definitely a factor in the receipt of erroneous entitlement payments. Also evident in that report is the need for information sharing and data collection. The following are listed as limitations to detecting and preventing fraudulent activity.

> **Limitations on data sharing.** Data collected by one federal agency could often be used to independently verify data for another federal agency but is not accessible, often because of congressionally mandated prohibitions. For example, HUD's subsidized housing programs could reduce improper payments by having access to National Directory of New Hires data, but HUD is not among the entities specifically permitted access to this database.
>
> **Limited data collection.** Much useful data is not currently collected at all during the course of normal program administration, or is not stored in a way that it can be retrieved, isolated or sorted.
>
> **Inherent conflict between promptness and accuracy.** Programs that require very quick payment processing, such as emergency benefit programs, will invariably sacrifice some preventive application review procedures.
>
> **Inherent conflict between privacy and data collection needs.** Some data that would be useful in preventing or detecting erroneous payments (Social Security Numbers, for example) will not be collected or used because of individual privacy or business proprietary concerns. (www.cfoc.gov, November 26, 2002)

Access to Immigration Benefits Including Employment
Fraudulent documents are presented to gain immigration benefits such as employment, naturalization, and permanent residency status (green cards). The indictment of Jessie Issac, who ran an immigration consulting business, illustrates how fraudulent documents allowed individuals to obtain illegal immigration benefits.

> The indictment also alleges that Isaac, together with associates and various business entities, presented and caused to be presented various false statements in forms seeking, in some cases, H-1B visas, a nonimmigrant visa initiated by an employer for a foreign national working in a "specialty occupation." Other false statements and documents related to Alien Employment Certifications, which enable domestic employers to hire foreign nationals, and permit them to become permanent residents, if they work in fields for which there are insufficient, qualified U.S. workers. For example, Isaac submitted documents asserting that foreign nationals would be employed by one of his purported businesses in a specific job, at a specific location, at a specific salary, and for a specific length of time. (Immigration, September 26, 2002).

Access to Secure Facilities
Senator Max Baucus, Ranking Member of the Committee on Finance, in his report on driver's license fraud, addressed the access which a fraudulently obtained driver's license affords a criminal or terrorist.

> But why is the issue of identification fraud important? It is worth remembering that seven out of the 19 September 11th hijackers fraudulently obtained authentic driver's licenses

> through the Virginia Department of Motor Vehicles. They used these authentic driver's licenses to board the planes on that tragic day… A driver's license is a commonly acceptable form of identification. It also plays an integral role in helping to protect our national security. Not only are licenses used to board airplanes, they make it possible to re-enter the United States, obtain access to government buildings, open bank accounts, cash checks and buy weapons. What is most important about a driver's license is the apparent legitimacy it establishes (Baucus, 2003).

Similarly, Ronald Malfi, in his testimony before the Committee on Homeland Security, reported that the Office of Special Investigations created fictitious identities and fraudulent documents which they then "tested" to see what access could be gained. They found that:

> …counterfeit identification can be used to gain access to federal buildings and other facilities. In March, 2002, we breached the security of four federal office buildings in Atlanta using counterfeit law enforcement credentials to obtain genuine building passes, which we then counterfeited…They then were able to move freely throughout the buildings during day and evening hours. In April and May, 2000, we similarly gained access to numerous federal buildings in Washington, D.C., that contained the offices of cabinet secretaries or agency heads.

Timeline

The identity fraud process may take as long as two years or may be facilitated more quickly by skipping an access phase. A "fraudulent" United States passport or driver's license, for example, may be the only source of identification necessary to open bank accounts and set up the financial network necessary to enable the criminal activity.

Phase III: Using a Credible Identity to Facilitate Criminal Activity

Terrorism

According to the FBI's report, *Terrorism in the United States 1999*, terrorism is defined by the Code of Federal Regulations as "'the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (28 C.F.R. Section 0.85)." The Department of State chose Title 22 of the United States Code, Section 2656f(d) as the definition of choice for its publication *Patterns of Global Terrorism 2002*. "The term 'terrorism' means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience." While the definition may vary, a crucial factor in recent acts of terrorism is the use of identity fraud to open many avenues of infiltration and funding. In the case of the 9/11 terrorist attacks, several of the terrorists are alleged to have used fraudulent identification documents such as drivers' licenses, stolen credit cards, fictitious and/or temporary addresses, false passports and other fraudulent travel documents, and fictitious Social Security Numbers.

> The Justice Department scorecard since Sept. 11 includes 237 criminal charges lodged in terrorism investigations, more than 500 deportations linked to the Sept. 11 investigation, 18,000 subpoenas and search warrants issued, $124 million in more than 600 bank accounts frozen, and 1,228 secret wiretaps and searches approved on suspected terrorists or spies. (Atlanta Journal-Constitution, May 18, 2003)

On June 3, 2003, two members of a sleeper cell, "Abdel-Ilah Elmardoudi, 37, and Karim Koubriti, 24, were found guilty of conspiracy to provide material support or resources to terrorists, and of conspiracy to engage in fraud and misuse of visas, permits and other documents." (Detroit, June 3, 2003) It is reported that a questionable witness in the trial, Hmimssa, said that Elmardoudi wanted to get a certain Algerian into the United States so that he could attend flight school. (The Philadelphia Inquirer, June 4, 2003)

In his testimony before the Subcommittee on Social Security of the House Committee on Ways and Means on November 1, 2002, Hon. James G. Huse, Jr. Inspector General, Office of Inspector General, Social Security Administration, stated, "What has become apparent … in all of our work on the national investigation, is that a purloined SSN is as useful a tool for terrorists as it is for identity thieves" (Huse, 2002). Dennis Lormel, Chief, Terrorist Financial Review Group, FBI, in his testimony to the Senate Judiciary Committee Subcommittee on July 9, 2002, stated, "The threat [posed by terrorism and identity fraud] is made graver by the fact that terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated" (Lormel, 2002).

Money Laundering/Financial Crimes

Money launderers are intent on taking money they have gained through illegal means and depositing it in a bank or other financial institution, or using it to purchase insurance policies. When they withdraw the money, it appears to be coming from a legitimate institution and is, therefore, assumed to be "clean." Once a bank account is established, deposits and withdrawals can easily be made, especially if they are under the "red flag' thresholds. Insurance policies can be purchased and used as mutual funds, as in the Operation Capstone case. By over funding them, the criminals are then able to withdraw the majority of the money they invested as "clean funds." Clearly the ease with which an identity can be created contributes to money laundering schemes. While the U.S.A. Patriot Act requires financial institutions and insurance companies to verify the identities of their customers, a criminal can still use fraudulent documents. The FBI considers driver's licenses which are issued without adequate identity verification to be a matter of concern. "Criminal threats stem from the fact that the driver's license can be a perfect 'breeder' document for establishing a false identity. The use of a false identity can facilitate a variety of crimes, from money laundering to check fraud" (Pistole, 2003). The breeder document provides the identity verification and thus, the account or policy is opened and the money laundering can begin.

In a case in Boston in 2002, it became apparent that money laundering and identity fraud can be linked in another manner, as well. According to a December 11, 2002 article in *The Boston Globe*, several people were indicted on identity fraud, money laundering, conspiracy, and misuse of documents. The ring sold Social Security cards to illegal immigrants, who, in turn, used the false documentation to obtain legitimate Massachusetts driver's licenses. The perpetrators sold the Social Security cards for $2,500 and subsequently "laundered" their proceeds through banks and "front" businesses (Cambanis, 2002). Using false identity as the commodity to "earn" money that is then laundered is one more indication of the pervasiveness of identity fraud among the criminal element.

Drug Trafficking, Alien Smuggling, Weapons Smuggling

Identity fraud is a crucial element of alien smuggling, narcotics trafficking, and weapons smuggling. As noted in Part II, the INS intercepts many fraudulent documents, including border crossing cards, alien registration cards, and passports. According to a U.S. Department of Justice press release dated October 3, 2002, on "October 2, 2002, a United States District Court jury found Mohammed Hussein Assadi guilty of thirteen counts of illegally smuggling aliens from Iraq to the United States through Ecuador and Colombia" (U.S. Department of Justice, 2002). Evidence presented in the late 1997 trial showed the following.

> Using a loose network of associates, Assadi would recruit his "customers" in the Middle East or after they arrived in Ecuador, and for fees of up to $8,000 per alien would provide them with stolen and altered European passports – which do not require visas for entry in to the United States – and round-trip airline tickets to the United States in the names on the fraudulent passports. He would substitute the aliens' photos for those of the original passports' bearers, and instruct the aliens to alter their appearances to conform to the passports' nationalities. (U.S. Department of Justice, 2002)

According to Rand Beers, Assistant Secretary for International Narcotics and Law Enforcement Affairs, "There often is a nexus between terrorism and organized crime, including drug trafficking" (Beers, 2003). They form symbiotic relationships, as the drug smugglers are privy to the terrorists' weapons and military skills, while the terrorists get tips from the drug dealers about transfer and laundering illicit funds. They are able to help each other obtain fraudulent documents, such as passports and customs papers, that are necessary for border access. In a 1998 General Accounting Office report on identity fraud, it was noted that the United States Postal Service stated that identity fraud is used to finance drug trafficking. "Mail theft and credit card fraud activity frequently support drug trafficking. Large amounts of money may be obtained through such fraud" (Identity Fraud, 1998, p.37).

In early March 2003, six members of a terrorist cell operating in Charlotte, North Carolina were sentenced for racketeering and support of Hezbollah. The Bureau of Alcohol, Tobacco, and Firearms tracked and investigated the case which involved a multi-million dollar tobacco smuggling ring. Cigarettes were purchased in North Carolina, where the tax per carton is fifty cents, and transported to and sold in Michigan, where the tax was $7.50 per carton. The men, of course, kept the $7.00 per carton difference. According to an unidentified FBI agent quoted in a U.S. News and World Report article, "Here's a terrorist support cell that sets itself up in America's heartland. They have the ability to move people across borders and give them whole new identities. They have access to a constant flow of untraced cash, military training, and a network of criminal contacts to get weapons. That's not good news" (Kaplan, March 10, 2003).

Management of identity fraud has occurred on several fronts (see Diagram III-2). Legislation and regulation have attempted to define illegal conduct regarding the theft of personal identifiers and false documentation. Limited commercial information is available to authenticate identities. Information policies have been promulgated and technological solutions have been sought. Education and training of government and law enforcement personnel has increased. And finally, an awareness campaign has been launched to educate the public, as well as the private and public sectors on the significant problem of identity fraud.

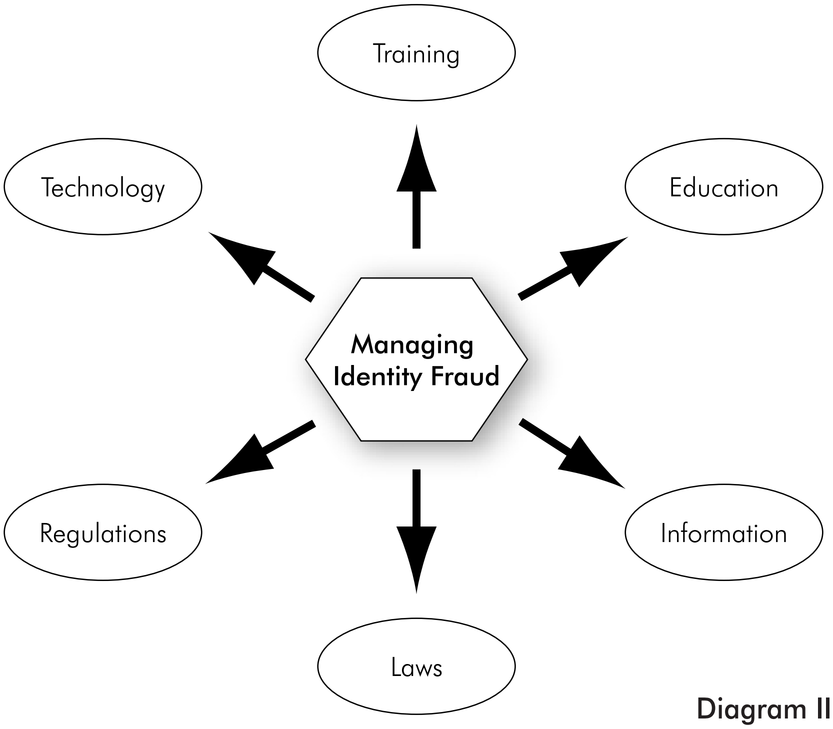


Diagram III-2
Managing Identity Fraud

Laws and Regulations

Current and proposed identity fraud legislation and regulation is spread across several agencies. Each current law or regulation has a specific intent regarding the mitigation of identity fraud, prohibits certain actions, and impacts upon certain agencies and/or industries (e.g. law enforcement, customs, airports, flight schools). Proposed laws and regulations may seek to amend or modify current ones in order to improve the success rate of investigations and prosecutions. They may also seek to address issues that are not currently covered by existing laws or regulations. Part IV discusses these legislative and regulatory issues.

Information and Technology

Policy defining the use, sharing, and distribution of information is in the formative stages. Resolution of issues of information sharing, privacy, and integration in a trusted system to ensure need to know distribution, as well as gaining greater access to domestic and global data are critical to managing identity fraud, Section V addresses these issues and proposes a model system.

Education, Training, and Awareness

Heightened awareness of the identity fraud problem through education, training, and the media has had an impact on the growth of identity fraud. Law enforcement and government personnel have been trained in visually identifying fraudulent documents. The public through the media, financial institutions, and non-profit organizations has received warnings and guidance on identity theft.

Conclusion

The pervasive nature of identity fraud as evidenced by the anecdotal cases noted here, as well as many others, will continue until a system is in place to control it. The system must be sophisticated, easily implemented, dynamic and global, so that it can be adapted to the newly designed methods the criminals and terrorists use to evade it. Unfortunately, devising such a system cannot occur easily or without challenges. Sections IV, V, and VI continue the discussion of the development, implementation, and challenges of an effective method of managing the risk of identity fraud.

♦♦♦

Part IV

Managing Identity Fraud: Laws and Regulations

Laws and regulations are a crucial component of managing identity fraud. In order to conduct investigations, make arrests and indictments, and successfully prosecute these crimes, the laws and regulations must cover the many permutations of identity fraud, alone and as a means to commit other crimes. Current domestic and international laws and regulations are spread across several agencies and cover many aspects of identity fraud and identity theft. Creating a data and information clearing house so that the severity of the problem can be measured and analyzed is difficult because of this. Several of the existing laws and regulations are covered in this section.

In the United States, the federal legislation that has been developed to address the identity fraud problem has focused on two means of risk mitigation; first, the criminalization of conduct relating to identity fraud; and second, the strengthening of tools designed to authenticate the identities of individuals. Comprising the first group are:

- The Identity Theft and Assumption Deterrence Act of 1998 (P.L. 105-318);
- The Internet False Identification Prevention Act of 2000 (P.L. 106-578); and
- The Secure Authorization Feature and Identification Defense Act ("SAFE ID Act," P.L. 108-21, Section 607).

The second group of laws, concerning identity authentication, is illustrated by the following:

- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT ACT") of 2001; Section 326, Verification and Identification; Section 403, Access by the Department of State and the INS to Certain Identifying Information in the Criminal History Records of Visa Applicants and Applicants for Admission to the United States; Section 405, Report on the Integrated Automated Fingerprint Identification System for Ports of Entry and Overseas Consular Posts and Section 414, Visa Integrity and Security.
- The Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173); Section 303, Machine-Readable, Tamper-Resistant Entry and Exit Documents;
- The proposed Fair and Accurate Credit Transactions Act (FACT Act), H.R. 2622; Section 207, Study on the Use of Technology to Combat Identity Theft.

Criminalization of Identity Fraud Activity

Since 1998, there has been a series of three laws enacted addressing different aspects of the identity fraud problem. Attempting to stem the flow of the ever-increasing numbers of Americans being victimized by identity thieves, Congress passed the Identity Theft and Assumption Deterrence Act of 1998. The principal components of this Act were the following:

- It amended 18 USC Section 1028, by adding the crime of Identity Theft, rendering it illegal for someone who "knowingly transfers or uses, without lawful authority a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." (Codified at 18 USC Section 1028 (a) (7)).
- It defined "means of identification" to include, as it relates to a specific individual: (A) identifiers such as name, Social Security Number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (B) biometric data, such as fingerprint, voice print, etc; (C) unique electronic identification number, address, or routing code; or (D) telecommunication identifying information or access device. (Codified at 18 USC Section 1028 (d)(7)).
- It enhanced the maximum penalty to 20 years imprisonment for a violation of 18 USC S1028, relating to fraudulent use of identification documents, and information, if done (A) to facilitate a drug trafficking crime…: (B) in connection with a crime of violence…; or

(C) after a prior conviction under this section becomes final. (codified at 18 USC Section 1028 (b) (3)).

- It mandated that the Federal Trade Commission establish a centralized procedure for logging complaints by victims of identity theft. (P.L. 105-318, Section 5).

The Identity Theft Act was followed by the Internet False Identification Prevention Act of 2000. Designed to address the "proliferation of websites that distribute counterfeit identification documents and credentials over the Internet," the Act rendered this activity criminal by expanding the scope of the federal fraudulent identification document crime to the "transfer of a document by electronic means." By this Act, Congress addressed the law enforcement dilemma of the Internet that, notwithstanding its significant benefit, it has become a haven for global crime, combining unbounded international reach with virtual anonymity.

Finally, last April, Congress passed the SAFE ID Act as part of the child protection law called the PROTECT ACT. Again focusing on the abuse of identification documents, Congress determined it to be a criminal offense when someone "knowingly traffics in false authentication features for use in false identification documents, or means of identification." (Codified at 18 USC Section 1028 (a)(8)). "Authentication features" was defined as "any hologram, watermark, certification, symbol, code, image, sequence of numbers… used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified." (Codified at 18 USC Section 1028 (d)(1).) In enacting the SAFE ID Act, Congress recognized the technical sophistication of the identity fraud perpetrator, who is able to make "desk-top published" dummies of breeder documents, such as birth certificates and driver's licenses, by faking or stealing government-issued embossed or foil seals.

Identity Authentication

The second category of federal legislation tackling the identity fraud problem has involved mandating, under certain circumstances, the development and use of different manners of identity authentication: information, biometrics and token-based. An example of an information and token-based identity authentication solution is that designed by the Federal agencies in response to Section 326 of the USA PATRIOT ACT.

Enacted in the weeks following 9-11, the USA PATRIOT ACT was designed to combat terrorism and the various criminal activities associated with it, including money laundering and identity fraud. Title III of the Act, entitled "International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001," required, at Section 326, Verification of Identification, that the Secretary of Treasury promulgate regulations setting forth the "minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution." (Codified at 31 USC Section 5318 (b)(1)). Section 326 further required that in prescribing the regulations, the Secretary of Treasury impose certain "minimum requirements" and that it take into consideration an enumerated list of "factors to be considered." With regard to the minimum requirements, the Secretary was obligated to require financial institutions to comply with reasonable procedures for:

(A) verifying the identity of any person seeking to open an account to the extent reasonable and practicable;

(B) maintaining records of the information used to verify a person's identity, including name, address, and other identifying information; and

(C) consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institutions by any government agency to determine whether a person seeking to open an account appears on any such list. (Codified at 31 USC Section 5318 (b)(2)).

With regard to the factors to be considered by the Secretary of Treasury in prescribing the regulations, the Act listed: "the various types of accounts maintained by various types of financial institutions, the various methods of opening accounts, and the various types of identifying information available." (Codified at 31 USC Section 318(b)(3)).

Following the Congressional mandate, the Department of Treasury, through the Financial Crimes Enforcement Network (FinCEN), developed with the seven federal financial regulators (the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS) the National Credit Union Administration (NCUA), the Commodity Futures Trading Commission (CFTC), and the Securities and Exchange Commission (SEC)) regulations implementing the identity verification requirement of Section 326. These regulations, promulgated as joint final rules on April 30, 2003, require that financial institutions develop a Customer Identification Program (CIP) that implements reasonable procedures to:

1. Collect identifying information about customers opening accounts, comprising at a minimum, name, address, date of birth, and a taxpayer identification number (e.g. a Social Security Number).
2. Verify that the customers are who they say they are. This can be through documentary means, such as a driver's license, or through a non-documentary, information means, such as that provided by a trusted third party.
3. Maintain records of the information used to verify the customer's identities.
4. Determine whether the customer appears on any list of suspected terrorists or terrorist organizations. (68 Fed Reg. 25090, 25113, 25131, 25149).

Financial institutions had until October 1, 2003 to fully comply with the Section 326 regulations.

Significantly, the Department of Treasury recognized the difficulty in authenticating the identities of foreigners in its October 21, 2002 Report to Congress. There, Treasury specifically found that,

> …there are significant impediments to domestic financial institutions' ability to identify, much less verify the identity of, foreign nationals. The wide disparity in identification documents, the pervasive problem of fraudulent identification documents, and the fact that many foreign nationals who establish accounts in the United States are not physically present here mean that it might not be practicable for Treasury to prescribe rigid rules of acceptable or unacceptable forms of identification. (Department of Treasury, 2002, p. 3)

Although undoubtedly true, the Department of Treasury's search for a solution would be greatly enhanced if there existed global data, of a type and in a form, used to authenticate the identities of U.S. citizens through information-based identity authentication solutions.

Although well-intentioned, the Section 326 Customer Identification Program regulations are not sufficiently stringent to authenticate an individual's identity. By requiring only the submission of a document such as a driver's license to establish identity, the regulations are woefully ineffective. It has been widely conceded that driver's licenses and similar credentials are easily counterfeited or obtained fraudulently. In the absence of reliable credentials, the only practical solution must be to employ an information-based authentication system.

The other laws imposing requirements for the development and use of authentication tools to combat identity fraud generally focus on the application of biometrics and tokens. Most of these laws concern authenticating aliens. In the USA PATRIOT ACT, Section 403(c) required the Attorney General and the Secretary of State to utilize the National Institute of Standards (NIST), and to consult with the Secretary of Treasury, other Federal law enforcement and intelligence agencies, and with Congress, in the development and certification of a technology standard:

> [t]hat can be used to verify the identity of persons applying for a United States visa or such persons seeking to enter the United States pursuant to a visa for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name or such person seeking to enter the United States pursuant to a visa.

Although Section 403(c) of the USA PATRIOT ACT required the authentication of the technology standard within two years, or by October 26, 2003, more recently Congress imposed additional requirements on the Attorney General, the Secretary of State and NIST, regarding the development of biometrics-based authentication of aliens.

On May 14, 2002, the Enhanced Border Security and Visa Entry Reform Act of 2003 was passed. At Section 303, this Act imposed on the Attorney General and the Secretary of State the requirement that by October 26, 2004, they issue to aliens, "only machine-readable, tamper-resistant visas and entry documents that use biometric identifiers." In addition, they are obligated to establish "document authentication standards and biometric identifiers standards to be employed on such visas and other travel and entry documents from among those biometrics identifiers recognized by domestic and international standards organizations." Finally, the law required the Attorney General, in consultation with the Secretary of State, to install at all ports of entry of the United States equipment and software to allow biometric comparison and authentication of all United States visas and other travel and entry documents issued to aliens, and passports issued pursuant to the visa waiver program.

Most recently, Congress has focused on biometric authentication while undertaking the issues associated with reauthorization of the Fair Credit Reporting Act. With the support of the Bush Administration, the House has proposed a bill containing reauthorization, which also recognizes the need to address identity theft. In the proposed Fair and Accurate Credit Transactions Act of 2003, H.R. 2622, the sections of Title II, "Identity Theft Prevention," are designed to combat identity theft. Although most of the sections protect or empower the consumer in the credit environment, one specific section is designed to enhance identity authentication. As written, Section 207, "Study on the Use of Technology to Combat Identity Theft," would require the Secretary of Treasury "to conduct a study of the use of biometrics and other similar technologies to reduce the incidence and costs of identity theft by providing convincing evidence of who actually performed a given financial transaction." In conducting the study, the Secretary of Treasury is directed to consult with the federal banking agencies, the Federal Trade Commission, representatives of financial institutions, credit reporting agencies, federal, state and local government agencies, the biometric industry, and other representatives of the general public. If the bill were to become law, the Secretary of Treasury would be required to provide a report, based on the study, within 180 days of enactment.

International Laws and Policies on Identity Fraud

In recent years, as in the United States, other countries have passed laws criminalizing identity theft. Again, as with the United States, there is very little indication that they have focused on the broader problem of identity fraud. Similarly, although some countries provide certain aspects of identity authentication, few countries require it as part of the defense against identity fraud.

In London, Home Office Minister Beverley Hughes announced a new offense to tackle identity fraud on June 18, 2003, in a speech at the Combating Identity Fraud Conference.

> This new offence will enable the police to crack down hard on criminals involved in identity fraud. False identities are commonly used by those engaged in organised crime and terrorism…The police usually have to rely on other linked crimes to get a conviction. The new offence will make it much easier and swifter for police to arrest criminals for identity theft as they will be able to arrest the criminals for just possessing fake or stolen documents (Home Office, June 18, 2003).

Home Secretary David Blunkett referred to the same offense, which will be part of an amendment to the Criminal Justice Bill due to be enacted later this year, on May 12, 2003, when he stated,

> Passport and driving licence fraud are gateway offences to organised crime and terrorism. Our legislation must keep pace with increasingly sophisticated criminals and complex crimes (Home Office, May 12, 2003).

Home Office Minister Lord Falconer stated, "These amendments send out a strong signal that terrorists and criminals cannot use identity fraud as a route to more serious crimes…They give the police the tools they need to stamp out abuse of the passport and driving licence application systems…" (Home Office, May 12, 2003).

The United Kingdom, much like the United States, is cognizant of the fact that current laws and regulations are not sufficient to combat the increasing problem of identity fraud and is role in terrorism, organized crime, and financial crimes. The new amendments to the Criminal Justice Bill are an effort to improve the laws and give law enforcement the power necessary to investigate identity fraud cases. The identity fraud proposals would allow police to arrest persons in possession of suspect documents immediately, rather than issue them a court summons for a later date.

The European Union does not have a statute that explicitly addresses identity fraud. The Commission of the European Communities is of the view that safeguards provided by the 1995 Privacy Directive and the 1997 Privacy Directive for the Telecommunications Sector adequately safeguard personal information (2002 OJ C 301). Further, the Commission considers computer access of consumer personal data and credit card numbers to be punishable under its Cybercrime Convention (*Id*.). Some individual European countries have laws governing identity fraud.

In the Netherlands, forging identity documents and conviction thereof, can result in a five year sentence. The Netherlands police maintain a large database of lost or stolen identity documents, called the Verification of Identity System (VIS).

> Details of around six million documents are held on the central database. Details are recorded for identity documents (mostly driving licences and passports), which have been reported lost or stolen. Whilst the majority of documents recorded are Dutch, details of documents issued

> in other countries are also held. Details of deaths are also held in case someone tries to assume the identity of a deceased person. The database can also be used to validate some of the data recorded on a document. This includes validating the "country code" and the number of digits used on a passport (Cabinet Office, July 2002, p. 38).

Belgian citizens are required to carry government issued identity cards. They also must register their address with the government and are subsequently visited by a government official to validate that the address is real. (Cabinet Office, July 2002, p. 39) In Finland, national identity cards are optional, but each person has a government number which holds governmental information about the person and which is stored in a database that government departments use to verify information and identity duplicate requests. (Cabinet Office, July 2002, p. 40) Denmark also maintains a database of its citizens, who each have an identifier number. Danish citizens are required to notify the government of a change of address so that the database can be updated. (Cabinet Office, July 2002, p. 40) The Republic of Ireland has signed a Memorandum of Understanding with the United Kingdom for increased sharing of document information. (Cabinet Office, July 2002, p. 41) In France, "Legal restraints forbid the exchange of personal information between government departments and private and public sector organisations – unless a judicial investigation is underway, in which case disclosure of information is mandatory" (Cabinet Office, July 2002, p. 41).

Canada prohibits identity fraud-related crimes via a plethora of statutory provisions, including personating a police officer (Criminal Code of Canada [CCC], § 130), theft (CCC § 322), credit card forgery or falsification (CCC § 342.01), false pretence or false statement (CCC § 362), telegram in false name (CCC § 371), fraud (CCC § 380), personation with intent (CCC § 403), personation at examination (CCC § 404), and acknowledging instrument in false name (CCC § 405). Canada does not have a national identifier that can be compared to the American Social Security Number. Citizens can apply for and obtain a Social Insurance Number (SIN), but those numbers have been used fraudulently in numerous cases. Proof-of-identity is required and it is illegal to apply for a second SIN. The government has taken steps to ensure that those checking identity documents are well-schooled (Cabinet Office, July 2002, p. 37). In November 2002, Immigration Minister Denis Coderre called for a national debate on the issue of instituting a Canadian national identity card. In a speech before the Standing Committee on Citizenship and Immigration on February 6, 2003, titled "Why Discuss a National Identity Card?" he stated,

> In the aftermath of the terrorist attacks in the United States on September 11, 2001, identity has taken on new prominence in countries around the world. Canada has been no different. Canadians have come to see the ability to establish identity as an important element of personal and collective security. And while the new focus on a positive proof of identity is partially rooted in the aftermath of the terrorist attacks, other forces are at play. Identity theft is seen as a serious and growing problem in Canada. Yet, as we sit here today, there is no specific crime of identity theft in the *Criminal Code* (Coderre, February 6, 2003).

Conclusion

As noted in Parts II and III, a means of managing identity fraud is essential. Unfortunately, identity fraud is pervasive in our society; if left unchecked, it will erode personal safety and economic soundness. A comprehensive, shared reporting database of information regarding identity theft and fraud cases is one step in the management of identity fraud. Another step is the promulgation of laws and regulations, both domestic and globally, that will lead to the enforcement, detection, and prosecution of criminals using identity fraud as a stand alone crime or as a facilitator of any number of other crimes. While the United States has several laws and regulations in effect, they tend to deal with the problem in a piecemeal fashion, rather than attacking the big picture. Section 1028 of Title 18, which has been amended several times, attempts to cover all aspects of producing and using fraudulent documents, but does not address the need to authenticate identity documents. The USA Patriot Act does a more thorough job of requiring systems for identification verification and for sharing identity information. However, regulations such as the Customer Identification Program are watered down and reduce effectiveness. Some of the proposed legislation, notably the Fair and Accurate Credit Transactions Act of 2003, continues the trend of addressing small pieces of the problem, which will not, in and of themselves, be effective in reducing identity fraud as a crime facilitator.

Federal and state legislative bodies must ensure that investigators and prosecutors are armed with adequate weapons to apprehend and punish those who commit identity fraud. As the trend toward greater information sharing and the use of relational databases becomes more prevalent, the ability of law enforcement and private sector fraud investigators to uncover identity fraud schemes through data analytics and link analysis technologies will become critical. A critical component of those technologies is the ability to make connections between seemingly unrelated events through the use of common identifiers, for example, Social Security Numbers. That ability would be significantly impaired by the adoption of certain pending legislation and regulations, such as preventing the use of Social Security Numbers for commercial or government transactions or requiring a unique individual identifier for health care records.

This problem is not unique to the United States; countries around the world are grappling with legislation that will protect privacy and security, but at the same time prevent the use of identity fraud. Some countries, notably the Netherlands and Finland, have developed databases with information on stolen identity documents and/or personal information that are shared among government agencies. Sharing information within and across borders, while maintaining a balance among risk, privacy, and security, presents a big, but perhaps not insurmountable, challenge to reducing identity fraud. Meeting this challenge is essential to successful global commerce.

♦♦♦

Part V
Managing Identity Fraud: Information Policy and Technology

As is evident from the preceding sections of this paper, identity fraud is a problem that needs to be stopped – easy to say, tough to accomplish. Identity fraud is pervasive in our society today and easily cuts across many different criminal and terrorist activities. Since the beginning of civilization there has been a crime problem and society has continually had to adapt its methods of preventing and detecting it, as well as swiftly bringing perpetrators to justice. However, as our society's knowledge and use of technology has grown and improved, a cultural change has taken place. At one time, not that many years ago, a breeder document, i.e., a driver's license, meant something; it could be used to establish a person's identity with little or no question. Now, technology has enabled criminals to produce fraudulent documents which can be used to procure legitimate documents – breeder documents. Counterfeit documents, such as credit cards, used to be easily detectable; now it is relatively easy to produce a counterfeit hologram that passes for the real thing most of the time. The technology and the ability of the criminal element to adapt and defeat systems that have been put in place by law enforcement, government, and industry have made it very difficult to authenticate a person's identity. Furthermore, the lack of significant domestic and global data has made it difficult to establish an effective information-based authentication system. Without the ability to make accurate assessments of identity, the integrity of our society comes into question. Managing the risk of identity fraud is necessary to shore up that integrity. We need the policy, technology, and commitment of government and industry leadership in order to return to a time when we can verify, validate, and authenticate that a person is who he says he is.

Applying Information-Based Methods to Determining Identity

Risk Management

The assessment of the threat or harm to an asset and the degree of protection taken to prevent it are the main components of risk management. In this case, the use of identity fraud enables harm or threat to an asset. For example, it has been shown that identity fraud facilitates terrorism, which is a threat to our national security. The amount of harm that identity fraud can cause (the threat), in terms of facilitating a terrorist risk, must be assessed. Once that is done, the level of protection needed to prevent it is determined. The assessment of the potential threat is balanced against the risk management strategies required to protect those assets.

The use of information-based risk management methods for credit purposes has been pioneered by the financial services industry. By performing credit reviews before approving loans or granting credit cards, financial institutions have been able to reduce the risk of bad credit and fraud. The potential losses from credit card fraud or foreclosed loans are assessed and protections are put in place that are commensurate with the amount of money that is at risk. Efforts to comply with Know Your Customer regulations, such as those delineated in the USA PATRIOT Act, have spurred the development of new techniques. The process of determining or authenticating identity using information can benefit from proven risk management methods. The levels of risk management required to support identity authentication, verification, and validation are based on several factors including risk, cost, speed of decision making, availability of information, and the sophistication of the individuals/organizations making the threat. Generally speaking, as the risk or threat increases, more sophisticated methods of risk management must be employed. Accordingly, as the risk increases, so does the cost to assess it, as more data/information and faster decision making is required. The methods of preventing the threat of identity fraud – i.e. more sophisticated risk management – must be geared to the sophistication of the criminals, whose means of creating breeder documents and a credible identity continue to become more complex.

Levels of Risk Management in Determining Identity

Determining the identity of a person in a routine transaction can be as simple as matching two identity documents, e.g. a driver's license and a credit card, to see that the name and address are the same. However, as has been shown, in the case of identity fraud, such documents are easily procured through the Internet, from counterfeiters, or by using a fraudulent document to acquire a breeder document. Therefore, other means of determining identity must be employed.

Level One: Validation

Information-based identity authentication begins with validation. Although it is the lowest level of risk management, it serves two important purposes: to determine if the identifying information presented by an individual, i.e. the identifiers, is not fictitious and to confirm that it conforms to an established format. In checking to see if the information is real, that is, not fabricated, a table or schedule of records is consulted. If the identifier provided by the individual, such as an address, phone number, or data birth, satisfies an existing logic or format then the identifier is considered to be "real."

Validating an identifier for format involves checking to see if the data set presented matches the code or order established for that particular identifier. For example, a MasterCard number always begins with the number 5. A Social Security Number's first three digits are determined by the state in which the card was granted. If a person claims to have been born in California, but presents a Social Security Number beginning with 040, a number issued in Massachusetts, further analysis may be warranted. A question to be asked in validating identifiers is, "Is the format or code of a particular identifier consistent with the format or code for that particular identifier?" If it is, and if the identifier has been matched, then the identifier is validated.

While validation provides an analyst with information on which to base a decision, it has limitations. If an identity fraud perpetrator understands how the system works, he or she will be able to produce false identifiers whose elements will not be revealed through the validation process.

Level Two: Verification

Using an information-based system, the next level of identity authentication is verification. Verification provides a risk analyst with more information on which to base a decision. Identity verification determines if the identifiers provided by an individual belong together, as distinguished from validation, which examines identifiers in isolation. Through parallel searching of multiple databases, such as public records, change of address, and phone numbers, the accuracy of the identifiers can be determined. For example, if a person supplies his name, address, phone number, and Social Security Number on an application, a search is constructed to confirm whether all four identifiers appear in the given combination in several databases. The verification process asks the question, "Do the identifiers in the given combination (e.g. name, address, phone number, Social Security Number) match the data as it appears in multiple databases?'' If the answer is yes, then the identifiers are considered verified.

If discrepancies appear in the database search, more analysis is necessary. Databases must be evaluated; those with the most current, accurate, and encompassing data are generally considered better. However, because of the cost associated with using the more comprehensive databases, their use has to be balanced against the need for precision in the risk assessment process. If the particular risk for which the verification process is being applied is low, databases with less information, and a corresponding lower cost, are sometimes considered sufficient. Conversely, if the risk is extreme, the combined use of government, commercial, and industry data may be warranted to manage the risk. The determination of which databases are eventually used in a given application is often an iterative process requiring continuous monitoring of the effectiveness of the overall identity authentication program.

In both the validation and verification processes, risk inherent to an identifier itself can sometimes be determined. Checking an identifier against an address, phone number, or Social Security Number validation database may unveil risk indicators. For example, if an address matches a prison or a commercial mail receiver, the address would be considered a high risk. If a phone number provided by an individual were for a pager or a disconnected line, the risk might be considered to be lower by a trained analyst. If the Social Security Number database shows that the number is associated with a deceased person or more than one person, further management of the risk is essential.

Level Three: Authentication

Although somewhat confusing, the third level of an information-based identity authentication process is referred to as "authentication." Authentication builds on validation and verification. The primary element of authentication is a modeling and scoring engine that is used to help determine the probability of the claimed identity of an individual being real. The authentication engine models and scores the identification information presented by an individual. In the authentication scoring process there are three potential scores: an affirmative score, meaning the person's claimed identity has been authenticated based upon the rules set for the application; a negative score, representing an unsatisfactory authentication score; and an "exception" score, meaning the process is inconclusive on authentication, usually necessitating further review by the entity applying the identity authentication process.

A modeling and scoring engine for identity authentication would work in much the same way as a credit model and scoring engine used by financial institutions. While a credit scoring engine, determines the level of financial risk of an individual, an identity decision engine determines the authenticity of identity, based on variables, including but not limited to:

- Existing records for that identity (validation)
- Consistency of internal codes (validation)
- Given identifier combination across databases (verification)
- Name
- Name variation/spelling
- Known aliases
- Address
- Phone number
- Social Security Number
- Immigration status
- Date of issue. (See Table V-1.)

The identifiers provided by an individual are analyzed to determine which of these variables apply. The information gathered about those variables is then matched against the information in several high quality databases and a score is assigned. Again, as is the case with a credit score, which predicts the creditworthiness of an individual, the identity score predicts the authenticity of the individual's claimed identity. The prediction is made by comparing the identity to similar patterns in an information repository.

Authentication is not without challenges. An identity decision modeling and scoring engine must be developed based on the process described later in this section. The information against which the variables may need to be checked could involve numerous databases, some of which are only available from an international source. This is of particular concern when the individual claims to be a citizen of a foreign country. Another challenge involves the processing of "exceptions," when further analysis by trained risk analysts is essential.

Identity Authentication Decision Model

While the process of authentication is logical and may seem simple, actually implementing the system is complex. In some cases, it includes building the model to predict behavior, developing a scoring process, procuring data or access to data for analysis purposes, and the integration of the components into a decision system.

In order to develop an identity decision modeling and scoring engine, three steps have to be taken. In step 1, analysts must assess a random sample of documents analyzed to identify aspects that relate to their authenticity and in so doing, choose the variables against which the information

Table V-1
Explanation of Identity Decision Model Variables

(This is not an exhaustive list)

Existing records for that identity Does the information provided match an existing record in a database?
Consistency of internal codes Does the data set match the established code or order for that particular identifier?
Given identifier combination across databases Do the identifiers in the given combination match the data as it appears in several databases?
Name Does the name provided match the records against which it is checked?
Name variation/spelling If there are variations in the name and/or spelling, do they meet the criteria for matching, i.e. same address?
Known aliases Has the name been used as an alias?
Address Does the address exist? Is it residential or commercial? Is it a correctional facility?
Phone number Is the phone number active? Is it for a landline, cellular line, or pager?
Social Security Number Does the number belong to more than one person? Is there any information associated with the number?
Immigration status Is there an immigration status associated with the identity presented in the breeder document? Does the breeder document address match the address provided at the time of immigration?
Date of issue When was the identifier (e.g. Social Security Number) issued? Does it make sense given the age of the person supplying the information?

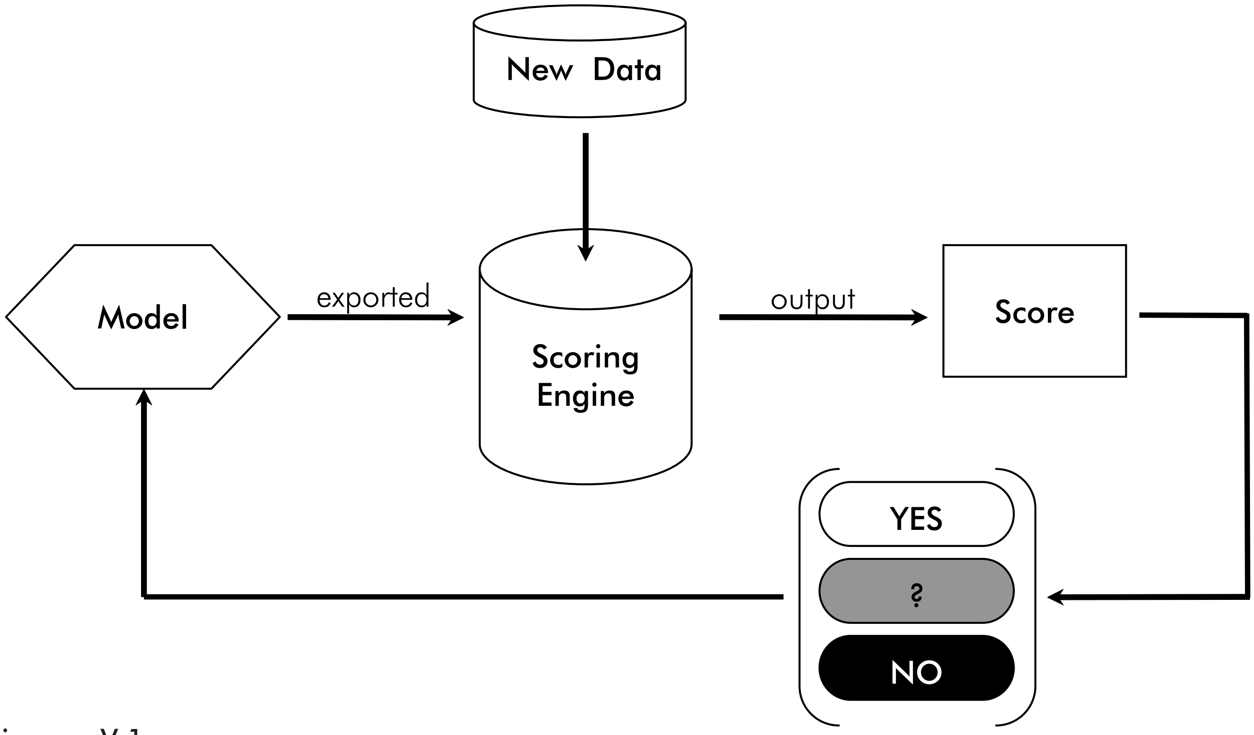


Diagram V-1
System Testing and Improvement

on the breeder document is matched and determine the decision-making process (analyst knowledge). In the next step, each of the variables is assigned a value (*weight*) based on how strong a predictor it is of a real identity, so that the document in question can be scored. In the third step the engine is continuously updated based on ongoing outcomes (outputs).

Diagram V-1 depicts how the system is tested and improved. New data is introduced to the system. The engine takes the existing model, a data set, and the new input, and produces a set of scores for records in near real time. This output is then used by the model to improve its decision making ability. The score is set up to provide an authentication of the identity, rejection of the identity, or an exception. A risk analyst then reviews exceptions to render a decision.

The full decision model is presented in Diagram V-2. A document is presented to the system to be scored. The scoring engine, which includes the latest version of the model, checks the document against data stored in the information repository and/or sends a request from the repository to specialized databases to gather the necessary information. (The system is constructed in this manner because it is not feasible or desirable to store all the data in one mega database.) The scoring engine scores the data on the document using the model and the data retrieved. It therefore uses existing data and past outcomes to predict future actions. If the response is ″yes,″ to authenticate the person or “no,” not to authenticate, the message is sent to the entity making the request. If the score falls in the exception range, an analyst reviews the output and reports to the entity. The system uses each decision to learn and improve the model.

The scoring engine must be reviewed and revised regularly to ensure that the variables and weight assessed each is appropriate. The validity of the system is crucial in terms of it producing fewer false positives and false negatives. A false positive decision is one where the system does not authenticate the identity when it should. In a false negative decision, the system authenticates the identity when it should not.

However, while an identity authentication decision model may be effective, its use is dependent upon it meeting privacy and security requirements. The next section presents a trusted technology solution that adds these two features to the identity authentication model.

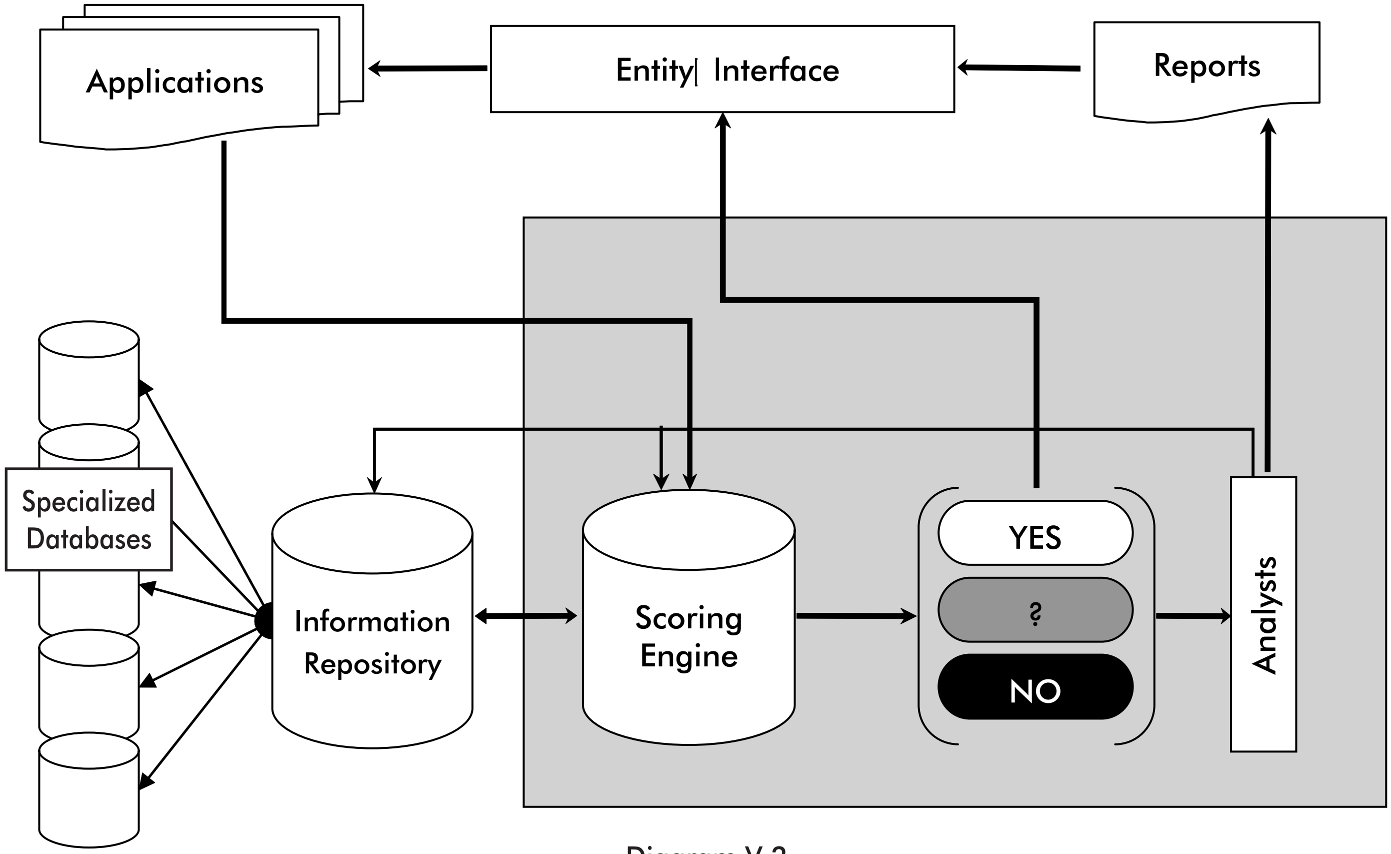


Diagram V-2
Databases: Authentication and Intelligence

A Trusted System

For a trusted identity authentication decision-making system to be accepted, it will require new technology and policy development. The trusted system must:

1. Protect the digital data.
2. Not store vast amounts of data, but be able to gather data when it is required from a vast number of domestic and global databases. ("What kind of data should be available and in what format should it be shared?")
3. Maintain the privacy of the information; responses to requests should validate, verify, or authenticate the person, but not necessarily include the particulars of the data.
4. Distribute data on a need to know policy-based, technology driven basis – individuals receive information based on their status in the system. ("Who will have access to the data and for what purpose?")
5. Log all activities so that they are auditable in near or real time and proper oversight can be maintained.
6. Adhere to legal and regulatory standards.
7. Be technically sound.

Trusted System Example: Radiant Trust™

A trusted identity authentication decision-making system that meets the requirements above is currently being developed. Building on Radiant Mercury™, a system used by DoD and other agencies to share data across security domains, Lockheed Martin is developing Radiant Trust, a system that provides customized message filters and distribution based on message content and rules, e.g. one alert format to the INS officer vs. a different message to a station supervisor.

Radiant Trust appears to solve the technical requirements for a policy driven trusted system. It provides the ability to share data across different security level domains while maintaining the integrity of the higher security classification systems. Such a system allows information to be gathered from domestic and global sources, and enhances the protection of privacy of individuals. It provides a solution that may alleviate the legal constraints on information sharing, while eliminating the need to store large amounts of data at one source.

Even if Radiant Trust can solve the technical issues of such a system, there is still a trust factor that must be addressed. The only way such a system will be accepted, and not viewed as another "Big Brother" approach, is if there is close oversight through a strong audit capability. All input and output data and every user action on the system must be capable of being fully audited.

Information Sharing and Privacy Concerns

As has been discussed above, the more sophisticated levels of risk management require accurate and significant amounts of data from a variety of sources. The sources of domestic data are commercial, private, and government entities. In many cases, there is a need for global data as well. In order for effective identity determination to occur, the data from these multiple sources must be shared in a secure manner that protects privacy. In extreme risk cases it is essential that databases that traditionally are not available are made accessible. Accessibility differs from information sharing, in that using databases to match variables and discern discrepancies in a particular extreme risk situation may not require the disclosure of all of the information in the database. In fact, best practices should dictate using the minimal amount of data needed to satisfy the level of identity authentication required.

Sharing must occur on many levels, including within the private sector, within the public sector, between the private and public sector, and in some cases with global entities. In order to accomplish this complex process, issues of privacy, trust, and security must be addressed in the context of legal, regulatory, and technical issues. This can only be done in an environment where clear privacy boundaries are established, strong security exists, and the system is trusted as a result of audit and oversight.

♦♦♦

Part VI
Managing Identity Fraud: Challenges and Recommendations

Challenges to Managing Identity Fraud

Easy Access to False Identifiers

The proliferation of Internet websites, how-to manuals, and mail order businesses that enable individuals and organizations to create and/or steal identities is seemingly limitless. Many of the laws and regulations that have been passed have been directed at curtailing access to information and criminalizing such behavior. The effects of these efforts have been hard to measure, but the identity fraud problem does not seem to have subsided as a result. While the public has been made more aware of the possibility of having their identities stolen and thus, have begun to take precautions against it, the same is not true of identity fraud.

Recommendations such as eliminating the use of a Social Security Number or reissuing random numbers, do not resolve the problem. The core issue is not an existing or new identifier, but the inability to validate, verify, or authenticate the identity. It is costly to add new security features to documents, as they provide relief for only as long as it takes the criminals to defeat the new system. Numerous examples exist where fraud has dropped significantly after such a feature is introduced, only to have the criminals defeat it in a matter of months. When the hologram was introduced on credit cards in 1982, counterfeiting of credit cards was reduced dramatically. However, it was only a matter of time before facsimiles of holograms started to appear on counterfeit cards and the resultant losses began to rise.

The emphasis in this area should not be placed on how to reduce the information sources or the availability of purchasing breeder documents. Rather, the challenge is how to render these fraudulent documents ineffective.

Limited Data Analysis and Research

Our overall ability to answer incisive questions about the pervasiveness of identity fraud in our society is severely handicapped by the lack of a reliable, organized, and inclusive reporting system, that accurately reflects all reported and detected identity fraud, cutting across enforcement agencies at each level of government. Such a system would enable government agencies and private enterprises access to information, so that trends such as the use of identity fraud as a catalyst to other crimes could be identified. While parts of the puzzle have been assembled from a variety of such organizations, it remains divided and mismatched. Federal agencies and private organizations and corporations use different indicators of identity fraud and do not collaborate to present a uniform picture, while state and local agencies generally do not collect and/or report the identity fraud cases with which they have dealt. Without consistent, accurate, and shared information on identity fraud cases, development of a systematic mechanism that enables further research in this area will continue to be hampered.

The challenge in this area is to develop a strong research agenda, based on the classification, collection, and sharing of identity fraud data, which will provide direction for decisions on identity fraud policy.

Limitations on Information Sharing

Identity information data is available from various sources, including commercial, private, governmental, and the international equivalents of each. Commercial data includes credit reports, which are available for appropriate-use purchase. Data is also available commercially from companies such as LexisNexis and Acxiom which offer government and business information solutions. Private information data includes the records held by mortgage and credit card companies, which is not available commercially and is protected by laws and regulations. Governmental information data includes public records such as birth and death certificates and business records, which is available for a nominal fee and often without restriction.

For the most part, these sources do not share their data, with each other or use each other's data to construct a composite or complete picture of a personal or business record. Even within industries, such as insurance, credit card companies, and the like, information sharing is limited because of competition, legal and regulatory prohibitions, and the lack of a secure system to facilitate sharing. For the purpose of controlling criminal and terrorist activities, greater sharing among these entities (commercial, private, and government) must occur. Policies, laws, and regulations to this end must be fully articulated, balanced, and monitored to insure compliance. Additionally, a methodology and technology that would allow each entity to grant information requests from the others without having to provide an entire data set would encourage these groups to cooperate.

The challenge is to create more sophisticated networks, both domestic and global, through which information can be shared in a trusted environment and meet the needs of commerce, law enforcement, and national security, while enhancing the protection of the personal information of law abiding citizens.

Privacy and Information Security

Government or commercial use of an information-based authentication solution for managing an identity fraud risk requires consideration of the privacy interests of the individual whose information is being used. This is not a new consideration as laws such as the Privacy Act of 1974 and the Fair Credit Reporting Act, originally enacted in 1975, evidence. More recently, the regulations under the Gramm-Leach Bliley Act and the Health Insurance Portability and Accountability Act detail how important societal interests, such as fraud prevention and law enforcement, can be balanced with personal privacy interests, even when very sensitive personal information, such as financial and health, are at issue. However, in the United States, as distinguished from some places like Europe, the commercial acquisition and use of other types of personal information, such as most identifying information, are largely unregulated.

We in the United States have generally allowed free market concepts to dictate the development of best practices in the commercial acquisition and use of non-sensitive personal information. As evidenced by the almost universal existence of Internet privacy policies, this approach has worked. Also indicative of the success of the U.S. approach is the development of off-line privacy policies in the information solutions industry. An example of such a data use policy can be found at the LexisNexis web site.

Critical to the success of commercial privacy best practices has been the appropriate balance struck between the need for a particular information solution and the need to protect an individual's privacy interest in the information. To appropriately balance these interests is an important objective in devising identity authentication solutions to meet the risks of identity fraud harms. The success of privacy best practices has been achieved where they have adequately considered the following factors:

1. Effectiveness;
2. Proportionality; and
3. Limiting the risk of harm to the individual from the use of the individual's information.

Effectiveness, in the identity authentication process means the degree to which an identity authentication solution has managed a particular identity fraud risk. For example, in the credit card issuance environment, where the use of commercially available information-based identity authentication solutions have been used for several years, this process has been found to be highly successful in reducing the amount of fraud caused by the misuse of identities. It is assumed that similar successes can be achieved in other environments where identity fraud has thrived, such as terrorism, drug trafficking and alien smuggling.

Another aspect of effectiveness is the availability of other means to accomplish the purpose intended by the product that uses personally identifiable information. However, for such alternative means to be considered viable, they must be at least as effective, commercially usable and privacy sensitive as the solution under consideration. Again, using the credit card issuance scenario as an example, for other solutions to be considered viable, they must initially reduce the fraud caused by the misuse of identity during the credit card issuance. This factor alone eliminates any solution that requires use of a biometric or token-based identity authentication solution, since both potential solutions require a preexisting means of confirming the identity of an individual through a reliable universal credential, and no such document currently exists. Further, time constraints of the normal credit card issuance process precludes other potential solutions, such as traditional background checks involving contacting unbiased job or credit references. Therefore, at least in the credit card issuance process, not only has the commercially provided information-based solution been found to have been effective, there exist no other even potentially viable comparable solutions.

The second significant factor in the evaluation of the privacy impact of a product that uses personally identifiable information is proportionality. Essentially, this factor involves consideration of the need for a particular type of personally identifiable information in achieving the desired purpose. In evaluating this factor, consideration must be given to the societal benefit of the desired objective and the sensitivity of the type of information involved. For example, for identity authentication in the credit granting environment, commercial entities typically use several types of identifying information and one of them is the Social Security Number. The Social Security Number is deemed sensitive because of its propensity for being abused in some identity theft cases. However, it has been found during the credit card issuance process that its availability allows for a significant enhancement in the identity authentication process. Consequently, although the Social Security Number is a sensitive type of personally identifiable information, the importance of the social security number for fraud prevention preponderates in favor of its use.

The third factor, which focuses of limiting the risk of harm to the individual, generally requires consideration of the Fair Information Practices or FIP. The components of FIP are usually considered to be notice, choice, access, security and enforcement, although most privacy regimes also include consideration of limited data use and retention and allowance for individual redress.

These issues raise the challenge of striking the right balance between the competing interpretations of privacy and the means to protect it in a digital world.

Domestic and Global Policy

As discussed above, the principal focus of U.S. and international legislation, pertaining to identity theft and identity fraud, has been the criminalization of the misuse of identities and the imposition of tighter privacy and security requirements on the use of personally identifiable information. Even when particular legislation has promoted identity authentication, it has been biometric and credential-based, while, with limited exceptions such as Section 326 of the USA PATRIOT ACT, failing to recognize the need for information-based identity authentication solutions.

As demonstrated by the recent Federal Trade Commission Report, "Overview of the Identity Theft Program," it is unfortunately undeniable that that the identity theft problem, and by natural extension the identity fraud problem, continues virtually unabated. We need, to paraphrase Assistant Treasury Secretary Wayne Abernathy, to put into the hands of those institutions that need it more information about the identities of the people who seek to do business with an institution than an identity thief would have (Abernathy 2003). This is most definitely the case when the person is new to the institution and there exist no available or reliable biometric or token-based solutions to authenticate the person. This new or initial phase of contact is often referred to as "enrollment."

However, the ability to authenticate the foreign traveler at enrollment through the use of an information-based system, given the present state of public record availability, is virtually impossible. Enrollment authentication of the foreign traveler is dependent upon the availability of global information:

> Knowledge-based systems have been developed to aid in authenticating the identity of U.S. citizens. These systems access a wide number of identifiers in domestic public records through identification scores that verify information supplied by individuals seeking visas and other travel and identifying documents. This system has proven effective for U.S. citizens, but it has not yet been replicated for non-U.S. citizens because information from global sources is not collected at this time. The events of September 11th shed light on this deficiency, its relationship to homeland security, and the urgent need to acquire and integrate this data into useful systems to help authenticate and validate identity (Willox, 2003, p. 1).

Further complicating the matter, some international laws, such as the European Union Data Protection Directive, will not permit the exporting of personal information, except under very limited circumstances.

Although the breadth, and wisdom, of international privacy laws that completely prohibit data exportation for identity authentication purposes are beyond the purview of this paper, there is a means to accomplish identity authentication, while respecting the privacy regime of a given locale. It is to accomplish identity authentication at the origin of the data, while transmitting only the authentication score or result. By allowing the authentication process to occur within the country where the data resides, a country is free to examine and audit the authentication processor for compliance with that country's privacy laws, while not inhibiting necessary identity authentication.

In addition, as was shown in Section IV, global laws and regulations on identity fraud differ from country to country. Only selected countries were reviewed, which points to the fact that there has been no comprehensive study of existing identity fraud global laws, regulations, and remedies. Such a study would help lay the foundation for the sharing of information through treatises (Mutual Legal Assistance Treatises and extradition) and cross border laws.

Challenges in this area include developing a comprehensive legal and regulatory strategy and gaining an understanding of the global issues and their impact worldwide.

Dedicated Resources

Until the events of 9/11, identity fraud had not been a high priority in government or the private sector. As the problem continues to grow and there has been heightened awareness of its insidious nature, finding solutions to it has been given a higher priority and more efforts have been made to mitigate it. Successfully combating this problem will require a significant monetary outlay in order to fund the research to measure and understand the problem, establish a centralized identity fraud reporting system, create a trusted environment for information sharing, encourage the research and development necessary to produce a trusted identity fraud authentication system, purchase and implement this new technology, hire new personnel, and train the staff.

As has been stated in many parts of this paper, managing identity fraud will take a holistic approach, one that cannot be successful if done piecemeal. Acquiring sufficient funding to tackle this problem in this manner is a major challenge.

Leadership

Several good efforts are underway to reduce the impact of identity fraud, but they need to be brought together. A lack of strong central leadership inhibits this from occurring. Identity fraud has become a national and global problem. Once a problem has risen to that level, the government must take a central role in providing the leadership to help solve it. Inherent in that leadership is the need for a central forum through which issues can be resolved. As has been discussed throughout this paper, these issues are complex and dynamic.

The challenges are for the federal government to provide the leadership to bring the current efforts together and to create a forum through which consensus, best practices, and cooperation can be facilitated and developed.

Recommendations

In order to meet these challenges, we are proposing that a comprehensive national and global strategy to combat the identity fraud problem be implemented. The recommendations offered here are intended to lay the framework for the development of such a plan. High level federal government direction and funding are essential to this proposal. The federal government must make a commitment of both leadership and resources in order for the strategy to be realized. The components of the plan will work together to provide the data, research analysis, trusted environment, laws and regulations, and research and development necessary to manage the identity fraud problem by rendering fraudulent documents ineffective and allowing accurate assessment of identity, while enhancing the protection of privacy.

Comprehensive National and Global Strategy Recommendations

1. Gain a commitment from the highest levels of federal government to lead and fund a national strategy to combat the identity fraud problem.
2. Establish a central information database of identity fraud incidents.
3. Establish a national identity fraud research agenda.
4. Establish more sophisticated domestic and global information -sharing networks.
5. Conduct a study of existing domestic and global policies, laws, and regulations to determine best practices for combating identity fraud.
6. Enhance the protection of individual privacy and information ownership.
7. Improve information sharing systems that enhance identity authentication solutions while protecting privacy.

Recommendation 1: Gain a commitment from the highest levels of federal government to lead and fund a national strategy to combat the identity fraud problem.

Putting a national policy in place to combat identity fraud requires leadership from the highest levels of government, a White House directive, and a committee that brings together the key stakeholders to develop consensus and cooperation. White papers and other studies such as this should be used to educate individuals in Congress and various federal departments, such as the Department of Homeland Security, about the importance of organizing, facilitating, and funding the development and implementation of a national strategy. These individuals will need to convene a group of high-level government officials, private sector individuals, and academics whose responsibility will be to study emerging information challenges and make recommendations directly to the White House and Congress. Such a committee would drive the recommendations in this white paper regarding data analysis and research, privacy and security, limitations on data and data sharing, dedicated resources, and domestic and global policy. One of the committee's charges should be the development of standards and best practices that allow for the protection of privacy, while not inhibiting commerce or placing national security at risk. In order to meet its charge and goals the group will require appropriate funding. A model for this approach is the Transportation Security Administration's Office of National Risk Assessment (ONRA), which is developing terrorism risk management strategies, policies, and technologies.

Recommendation 2: Establish a central information database of identity fraud incidents.

A major barrier to determining the extent of the identity fraud threat is the absence of a centralized information collection and sharing mechanism for incidents of identity fraud. The Federal Trade Commission Sentinel Database, which contains consumer complaints of identity theft, is a model for the development of an identity *fraud* database. However, there is minimal systematized sharing of identity fraud case data horizontally among independent enforcement agencies on the same government level. Likewise, there is little systematized data sharing vertically, among different levels of government (i.e., federal, state, local). A comprehensive identity fraud classification system needs to be developed to systematically measure the size, scope, and impact of identity fraud. A database utilizing such a classification system would enable the effective coordination and normalization of identity fraud data on a national level, help perfect methods for recording identity fraud subset data, and establish a sound foundation for meaningful research that will enhance methods of identity fraud prevention and control. The development of a national database on identity fraud case information and a system for accessing and sharing the data holds great potential for the administration of several empirical studies.

Recommendation 3: Establish a national identity fraud research agenda.

1. Exploratory and Descriptive Studies to Record and Understand the Size and Scope of Identity Fraud

The national database, described above, will provide a central, normalized recording and reporting of incidents of identity fraud. Using the database, researchers will be able to produce statistics that will not just reflect criminal incident volume, but will produce aggregate figures on case-specific characteristics such as duration of offenses, monetary loss, association with other offenses, criminal methods, criminal behavior, and extent of identity fraud conspiracies. Comprehensive trend studies can be produced with an eye toward exploring emerging relationships among variables such as offender methods and financial damage resulting from the offenses. Additional studies, such as one focused on the impact of identity fraud on domestic and global commerce, will be possible.

2. A Study of Criminal Organizations Using Identity Fraud as a Facilitator

The development of a national database of identity fraud case information would allow research on individuals and criminal groups that perpetuate identity fraud as an enabler to the achievement of other criminal objectives (e.g., terrorism, alien smuggling, drug trafficking, weapons smuggling). Network analysis could be used to track relationships and assess the strengths of relationships among offenders and identity fraud ring organizations both nationally and internationally.

3. Effectiveness of Identity Fraud Investigation and Prosecution

A national database of identity fraud case information would be the source of a content analysis of identity fraud cases charged vs. those dismissed, isolating characteristics essential for successful case investigations. Likewise, discriminate analyses of identity fraud conviction rates could be conducted focusing on the effects of factors such as strength of evidence, complexity of cases, source of discovery, and inter-jurisdictional enforcement coordination, on the ultimate outcomes of identity fraud prosecutions. A similar global database would provide further information.

4. Identification of Characteristics of Victims

A comprehensive national database of identity fraud incidents would permit the examination of characteristics of individuals, agencies, and businesses falling victim to identity fraud offenders. In effect, aggregate data would allow research that isolates those characteristics and combinations of characteristics which create vulnerabilities precipitating identity fraud victimization. The results of such studies could be used to model risks and risk relationships that, if left unchecked, raise the probability of identity fraud victimization. This type of research would be especially useful, because it would optimize risk assessment of combinations of vulnerabilities which are strongly associated with identity fraud victimizations. This, in turn, would increase the effectiveness of validation, verification, and authentication strategies and systems.

Recommendation 4: Establish more sophisticated domestic and global information sharing networks.

The establishment of more sophisticated domestic and global networks will provide the requisite information for accurate validation, verification, and authentication. The following recommendations will facilitate the development of these networks.

Data Sharing Policies and Standards
Comprehensive policies, standards, laws, and regulations must be developed to define how personal information and records can be shared, who can have access to them, and under what circumstances they can be shared. Exceptions for detecting criminal behavior and national security purposes must be fully articulated.

Accessible Databases
Specialized domestic and global commercial, private, and government databases must be made available or created. These databases must provide personal identifier records that can be accessed by concerned entities, without jeopardizing privacy or the security of the data, and at the same time reducing liability and providing indemnification. This will require numerous agreements among governments, governments and the private sector, and private sector organizations. The United States government must take a strong central leadership role if this is to occur. As stated in section V of this paper, global data collection is much more of a challenge than domestic data and is critical for national security. Public private partnerships should be formed to help acquire or gain access to global data, especially data from riskiest parts of the world, to help protect borders and promote commerce.

Recommendation 5: Conduct a study of existing domestic and global policies, laws, and regulations to determine best practices for combating identity fraud.

It is necessary to complete a comprehensive study of existing domestic and global laws and regulations concerning identity fraud, data collection, and information sharing. The study should ascertain areas of ambiguity and gaps, review potential remedies, suggest methods of sharing data, and propose model identity fraud laws. These results should yield a best practices approach for managing identity fraud and be the first step in developing agreements for promulgating comprehensive laws and sharing data on a global basis.

Recommendation 6: Enhance the protection of individual privacy and information ownership.

Inherent in all of the recommendations proposed in this white paper is the goal of enhancing the protection of privacy. As solutions are developed to combat identity fraud, it is crucial to consider the enhancement of individual privacy and information ownership. Policies which require the protection of privacy while balancing the need for information sharing must be established. Inherent in such policies will be risk assessment, as well as the assessment of potential harms including, financial loss, personal safety, civil or criminal violations, and the unauthorized release of personal, government, or commercial data. Various technology and information industry groups, as well as government organizations such as the Department of Commerce's National Institute for Standards and Technology and the President's E-Authentication E-Government initiative, have proposed principles and standards and policies to address privacy and information sharing issues. These efforts can provide the framework for a comprehensive government and industry policy, if leadership is provided to incorporate them into a national policy.

Recommendation 7: Improve information sharing systems that enhance identity authentication solutions while protecting privacy.

Because the authentication of identifiers presented in the procurement of a breeder document is the critical stage in preventing identity fraud, an information-based authentication system is the only solution that truly works. While identity authentication systems currently exist, they are not robust enough nor do they provide the requisite privacy and information security that must be included in a trusted system. Therefore, the focus must be on the research and development of a trusted system (see Section V) that will effectively and efficiently authenticate identity, while maintaining the privacy and security of personal identifier information. Such a system will go a long way toward rendering fraudulent breeder documents ineffective. The design of the system must be such that it will enable decisions regarding identity to be made without hampering commerce or impacting on national security.

In order for the advanced identification authentication decision-making system to be accepted by the leadership committee members (Recommendation 1), there must be an oversight committee to monitor the use of such a system. The purpose of the committee will be to insure that the system is audited for accountability. New knowledge gained from the analysis of the information collected in a centralized database (Recommendation 2) and from research studies proposed in Recommendation 3 will improve the system's decision making process. The system will only be effective if large amounts of domestic and global data are made available through sophisticated information-sharing networks (Recommendation 4). The forging of these networks will be facilitated by the knowledge gained in studying existing domestic and global policies, laws, and regulations (Recommendation 5). This will result in developing global best practices to facilitate information sharing. Recommendation 6, "Enhance the protection of individual privacy and information ownership," is a central tenet of an information based identity authentication system. Absent this, the system will not be trusted and will not be accepted by governments, private sector entities, individuals and the organizations representing their interests, and other impacted constituencies.

Conclusion

As John S. Pistole of the FBI noted in his remarks before the House Select Committee on Homeland Security on October 1, 2003,

> The crucial element in the acceptance of any form of identification is the ability to verify the actual true identity of the bearer of the identification. In today's post-9/11 world, this element is all the more important because, in order to protect the American people, we must be able to determine whether an individual is who they purport to be. This is essential in our mission to identify potential terrorists, locate their means of financial support, and prevent acts of terrorism from occurring.

Identity fraud is a national crisis with global implications. Its pervasiveness must be recognized, especially as a facilitator of crimes that threaten national security, the economy, and personal privacy and security. If identity fraud is not seen as a significant and insidious threat, it will not be dealt with accordingly. Ronald D. Malfi's statement to the Committee on Homeland Security on October 1, 2003 indicates the enormity of the threat. He outlined the tests conducted by the Office of Special Investigations which showed that fraudulent driver's licenses and birth certificates were sufficient to gain entry to the United States from Jamaica, Barbados, Mexico, and Canada. During their investigation, they were able to purchase firearms in five states using counterfeit driver's licenses with fictitious identifiers. They were able to gain access to federal buildings, as well. "In March, 2002, we breached the security of four federal office buildings in the Atlanta area using counterfeit law enforcement credentials to obtain genuine building passes, when we then counterfeited. We were also able to obtain building passes that authorized us to carry firearms in the buildings" (Malfi, 2003). Malfi listed three conclusions: "(1) government officials and others generally did not recognize that the documents we presented were counterfeit; (2) many government officials were not alert to the possibility of identity fraud and some failed to follow security procedures and (3) identity verification procedures are inadequate" (Malfi 2003). Understanding and facing the threat of identity fraud is crucial to solving it. This white paper has focused on exposing the problems that Postole and Malfi discussed in their October 1, 2003 remarks. It continues further, however, and offers recommendations to help combat them.

The challenges to solving the problem are many. The key is to authenticate personal identifiers used to procure breeder documents, thus rendering fraudulent identities ineffective. Inherent in that challenge, however, is the need to classify, collect, and share identity fraud data, both domestically and globally, while enhancing the protection of privacy of individuals and meeting the needs of domestic and global commerce, law enforcement, and national security.

Meeting those challenges will necessitate strong national leadership in the United States, new methods of collecting and classifying identity fraud, a comprehensive research agenda, and an investment in the research and development of emerging and promising technologies. The same effort must be undertaken on a global scale to facilitate the formulation of best practices for combating identity fraud and enhancing information sharing.

Without a national and global strategy, identity fraud will continue to grow exponentially, as will the possibility of terrorist acts, financial crimes, drug trafficking, weapons smuggling, and alien smuggling, all of which have an adverse impact on the global community and commerce. The recommendations offered here are an attempt to manage identity fraud so that its growth will be contained and reduced. Inherent in the success of a strategy to do so is the commitment of the highest levels of government, both in terms of leadership and resources, which will facilitate the implementation of a research agenda and the development of an information database of identity fraud incidents. These, in concert with sophisticated information-sharing networks will lead to the development of a best practices policy and improved information sharing systems, which, in turn will enhance and enable identity authentication.

♦♦♦

References

The ABC news nuclear smuggling experiment: the journey of NRDC's uranium slug and the potential consequences. Nuclear Weapons and Waste: In Depth Fact Sheet. Natural Resources Defense Council. (2002, September 11). Retrieved May 12, 2003, from: http://www.nrdc.org/nuclear/furanium.asp

Abernathy, Wayne. (2003, April 10). The many ugly faces of identity theft. Speech delivered to the 2003 Banking Institute of University of North Carolina School of Law's Center for Banking and Finance, Charlotte, North Carolina. Retrieved September 26, 2003 from: http://www.ustreas.gov/press/releases/js177.htm

Agents with fake IDs again slip by border security, GAO says. (2003, May 14). Cox News Service. Retrieved June 11, 2004, from: http://www.azstarnet.com/border/30514nBORDER-FORGERY.html

Al-Qaida resurges as threat. (2003, May 18). Atlanta Journal-Constitution. p. 1A.

Baucus, Max. (2003, September 9). Statement of Senator Max Baucus Driver's License Fraud Oversight Hearing. Committee on Finance. Retrieved October 7, 2003 from: http://www.senate.gov/~finance/hearings/statements/090903mb.pdf

Beales, Howard. (2002, March 20). Identity Theft: The FTC's Response: Hearings before the Subcommittee on Technology, Terrorism and Government Information of the Senate Judiciary Committee. Retrieved May 9, 2003, from: www.ftc.gov/os/2002/03/idthefttest.htm

Beers, Rand. (2003, March 13). Narco-Terror: The Worldwide Connection between Drugs and Terror. Testimony before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information. Retrieved May 7, 2003, from: www.state.gov/g/inl/rls/rm/2002/8743.htm

Cabinet Office, United Kingdom. (2002, July). Identity Fraud: a Study. Retrieved June 22, 2003, from: www.homeoffice.gov.uk/docs/id_fraud-report.pdf

Cambanis, Thanassis. (2002, December 11). 6 Indicted in Identity-Fraud Ring. The Boston Globe, p. B2.

CFO-PCIE Improper and Erroneous Payments Work Group, Sub-Work Group on Indicators Final Report on Indicators. (2002, September 17). Retrieved June 9, 2003, from: www.cfoc.gov

Chin, K. (1999). Smuggled Chinese: Clandestine Immigration to the United States. Philadelphia: Temple University Press.

Coderre, Denis. (2003, February 6). Why Discuss a National Identity Card? Retrieved June 22, 2003, from: www.cic.gc.ca/english/press/speech/id-card.html

Cronin, Michael. (2002, October 9) Immigration Service Implements Anti-Terrorism Practices. Testimony before the Senate Judiciary Technology, Terrorism and Government Information Subcommittee. Retrieved June 6, 2003 from: http://www.usembassyjakarta.org/terrorism/imigration_service.html,

Customs statistics and accomplishments 2002. Retrieved May 11, 2003, from: http://www.customs.ustreas.gov/xp/cgov/toolbox/about/accomplish/accomplishments.xml

Department of Treasury. (2002, October 2). A Report to Congress in Accordance with 326(b) of the Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. Retrieved October 3, 2003 from: http://www.treas.gov/press/releases/reports/sec326breport.final.pdf

Detroit terror jury finds 2 0f 4 defendants guilty of conspiracy. (2002, June 3). CNN.com/Law Center. Retrieved June 6, 2003, from: http://www.cnn.com/2003/LAW/06/03/Detroit.terror.ap/index.html

Enhanced Border Security and Visa Entry Reform Act of 2002, P.L. 107-173.

Europol. (2002, October 3). 2002 EU Organised Crime Report, Public Version. File number: 2530-108 rev1.

Federal Bureau of Investigation. (1999).Terrorism in the United States 1999. Retrieved May 6, 2003 from: www.fbi.gov/publications/terror/terror99.pdf

Federal Trade Commission. In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act. Facts for Business. Retrieved June 18, 2003, from: http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

Federal Trade Commission. (2000, August 30) Identity Theft Complaints Triple in Last Six Months: FTC Victim Assistance Workshop To Be Convened October 23-24. Retrieved June 2, 2003, from: www.ftc.gov/opa/2000/08/caidttest.htm

Federal Trade Commission – Identity Theft Survey Report. (2003, September) Prepared by Synovate. Retrieved September 4, 2003 from: www.ftc.gov/os/2003/09/synovatereport.pdf.

Federal Trade Commission. (2003, January 22). National and State Trends and Identity Theft. Retrieved May 7, 2003 from: http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf.

Federal Trade Commission. (2003, September). Overview of the Identity Theft Program: October 1998 – September 2003. Retrieved September 26, 2003 from: http://www.ftc.gov/os/2003/09/timelinereport.pdf.

Finckenauer, J. O. and Schrock, J. Human trafficking: A Growing Criminal Market in the U.S. National Institute of Criminal Justice, International Center. Retrieved May 8, 2003, from: http://ojp.usdoj.gov/nij/international/ht.html

GAO: U.S. Inflated Terror Successes. (2003, February 21). CBSNEWS.com. Retrieved May 10, 2003, from: http://www.cbsnews.com/stories/2003/02/21/attack/main541518.shtml

Gramm-Leach-Bliley Act, Title V, P.L. 106-102 (Title V codified at 15USCS Sec. 6809, et seq.)

H. R. 3162. USA PATRIOT Act of 2001, P.L. 107-56.

Hoar, Sean B. (2001, March). Identity Theft: The Crime of the New Millennium. United States Attorneys' USA Bulletin, U. S. Department of Justice, 49:2. Retrieved June 12, 2003, from: http://www.cybercrime.gov/usamarch2001_3.htm

Holman, K. (1999, August 25) Airline drug bust. Retrieved May 8, 2003, from: www.pbs.org/newshour/bb/law/july-dec99/bust_8-25a.html

Home Office. (2003, June 18). New Offence to Tackle Organised Crime and Terrorism. Retrieved June 22, 2003, from: www.gnn.gov.uk/gnn/national.nsf

Home Office. (2003, May 12). Supporting Police in the Fight Against Crime and Terrorism. Retrieved June 22, 2003, from: www.gnn.gov.uk/gnn/national.nsf

H. R. 2035 (proposed). (2003, May 8). Identity Theft and Financial Privacy Protection Act of 2003. Retrieved June 20, 2003, from: www.theorator.com/bills108/hr2035.html

Huse, James G. (2001, November 1). Testimony before the Subcommittee on Social Security of the House Committee on Ways and Means, Hearing on Social Security Administration's Response to the September 11, 2001, Terrorist Attacks. Retrieved May 5, 2003, from: http://waysandmeans.house.gov/legacy/socsec/107cong/11-1-01/huse.htm

Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited, United States General Accounting Office. (1998, May). Retrieved May 7, 2003, from: frwebgate.access.gpo.gov/cgi-in/getdoc.cgi?dbname=gao&docid=f:gg98100b.pdf

Identity Theft and Assumption Deterrence Act, P.L. 105-318, 18USCS Sec. 1028(a).

Identity Theft: Greater Awareness and Use of Existing Data are Needed. (2002, June). United States General Accounting Office. GAO-02-766. Retrieved May 8, 2003, from: www.gao.gov

Identity Theft: Prevalence and Cost Appear to be Growing. (2002, March 1). United States General Accounting Office, GAO-02-363. Retrieved May 8, 2003, from: www.gao.gov

Immigration Consultant and Six Women Indicted in Visa Fraud Ring Alleging Sham Marriages. (2002, September 26). Press release United States Attorney, Northern District of Illinois. Retrieved June 11, 2003 from: www.oig.dol.gov/public/media/oi/jisaac.html

International Crime Threat Assessment. (2000 December). Retrieved August 29, 2003 from: www.fas.org/irp/threat/pub45270chap2.html

Kaplan, David E. and Monica M. Ekman. (2003, March 10). Homegrown Terrorists. U.S. News and World Report, 134:7, 30.

Library of Congress (2003, July). Asian Organized Crime and Terrorist Activity in Canada, 1999-2002. A Report Prepared under an Interagency Agreement by the Federal Research Division, Library of Congress.

Lormel, D. M. (2002, July 9). The identity theft penalty enhancement act. Statement for the record before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information. Retrieved May 12, 2003 from: http://www.fbi.gov/congress/congress02/idtheft.htm.

Major Provisions of the Aviation and Transportation Security Act. Retrieved June 12, 2003, from: http://www.aviationtoday.com/reports/timelines010202.pdf

Malfi, Ronald D. (2003, October 1). Counterfeit Identification Raises Homeland Security Concerns. Testimony Before the Committee on Homeland Security. GAO-014-133T.

Mixed verdict in first terror trial. (2003, June 4). The Philadelphia Inquirer, p. A01.

ONDCP fact sheet: Interdiction operations. (2002, January). Retrieved May 6, 2003, from: http://www.whitehousedrugpolicy.gov/publications/international/factsht/interdiction.html

Permanent Subcommittee on Investigations of the Committee on Governmental Affairs. (2002, February 4). Phony Identification and Credentials via the Internet. Retrieved June 11, 2003, from: http://216.239.39.100/search?q=cache:1HJSRy4Ssy8J:www.bna.com/webwatch/+US+s

Pistole, John S. (2003, October 1). Fraudulent Identification Documents and the Implications for Homeland Security. Statement for the Record Before the House Select Committee on Homeland Security. Retrieved October 1, 2003 from: http://www.fbi.gov/congress/congress03/pistole100103.htm.

Queens prosecutors indict 17 in alleged mortgage scheme. (2003, May 9). Retrieved May 12, 2003, from: www.newsday.com

Richey, W. and Blair, J. (1998, June 3). Smuggling: Not Just Drugs, Anymore. Christian Science Monitor, csmonitor.com. Retrieved May 7, 2003, from: http://csmweb2.emcweb.com/durable/1998/06/03/p1s3.htm

The SAR activity review – Trends, Tips and Issues. (2003, February). Bank Secrecy Act Advisory Group, 5. Retrieved May 6, 2003, from: http://www.fincen.gov/sarreviewissue5.pdf

Solomon, J. (2003, March 4). U.S. says it's foiled weapon smuggling. Associated Press. Retrieved May 11, 2003 from: http://highmarkfunds.stockpoint.com/highmarkfunds/newspaper.asp?Mode=Middle%2BEast&Story=20030304/063w2792.xml.

Stana, R. M. (2002, June 25). Identity Fraud: Prevalence and Links to Alien Illegal Activities. United States General Accounting Office, GAO-02-830T. Retrieved May 5, 2003, from: www.consumer.gov/idtheft/reports/gao-d02830t.pdf

Teamwork in Bangkok Dismantles Smuggling Ring Linked to Terrorism. (2002, May) CommuniQUE. U.S. Department of Justice, Immigration and Naturalization Service. Retrieved June 6, 2003, from: http://www.immigration.gov/graphics/publicaffairs/communique/may02_comm.pdf

Transaction Systems Architects (TSA). Money Laundering: What You Don't Know Can Hurt You. Trends. Retrieved May 9, 2003, from: http://www.tsainc.com/trends/loss_prevention.asp

Transactional Records Access Clearinghouse (TRAC). (2002, June 17). Criminal enforcement against terrorists. Retrieved May 3, 2003, from: http://trac.syr.edu/tracreports/terrorism/supp.html

United States Department of Health and Human Services. (2002, March 3). "Fact Sheet. Retrieved June 19, 2003, from: http://www.hhs.gov/news/press/2002pres/hipaa.html

United States Department of Justice. (2003, October 3). Iranian convicted of running profitable alien smuggling operation in South America. Retrieved June 4, 2003 from: www.usdoj.gov/usao/dc/press/02298.html

United States Department of State. (2003, April). Patterns of Global Terrorism 2002. Retrieved May 6, 2003, from: www.state.gov/documents/organization/20105.pdf

United States Department of the Treasury. (2002, July). National Money Laundering Strategy 2002. Washington D.C. Retrieved May 8, 2003 from: http://www.ustreas.gov/press/releases/docs/monlaund.pdf.

United States. Drug Enforcement Administration. (2003) Money Laundering, 2003. Retrieved May 4, 2003 from: www.usdoj.gov/dea/programs/money.

United States General Accounting Office. (1998, June). Money Laundering: Fincen Needs to Better Manage Bank Secrecy Act Civil Penalty Cases. Washington, DC: U.S. Government Printing Office.

United States General Accounting Office. (2000, May). Alien Smuggling: Management and Operational Improvements Needed to Address Growing Problem. Washington, DC: U.S. Government Printing Office.

United States General Accounting Office. (2003, January). Better Management Oversight and Internal Controls Needed to Ensure Accuracy of Terrorism-Related Conviction Statistics. Washington, DC: U.S. Government Printing Office.

United States v. Karro, 257 F.3d 112 (2nd Cir. 2001)

Willox, Norman A. (2003, August). Report on Government Need for Global Data. LexisNexis. Unpublished manuscript.

Willox, Norman A. and Thomas Regan. (2002) Identity Fraud: Providing a Solution. Retrieved June 22, 2003 from: www.lexisnexis.com/about/whitepaper/IdentityFraud.pdf

Yang, C.M. (2000, May 2). Gun Smuggling Ring Busted: U.S., Canadian Agents Seize 23,000 Guns and Parts. Retrieved May 8, 2003, from: http://abcnews.go.com/sections/world/DailyNews/gun_smuggling000502.html