



Released: October 2, 2001

IDENTITY THEFT: AUTHENTICATION AS A SOLUTION-REVISITED

BY: NORMAN A. WILLOX, JR.¹ AND THOMAS M. REGAN, ESQ.²

In March of 2000, in connection with the Identity Theft Summit convened in Washington, D.C., we examined the crime of identity theft and recommended a solution that commercial and governmental entities can, and should, employ that would help prevent the identity theft perpetrator from benefiting from identity theft.³ The solution, authentication, requires businesses, government and other entities providing valuable products and services to the public, to confirm the identification of the individuals whom they service, through the use of information pertaining to the individuals. We recognized that, under certain circumstances, authentication should be supplemented with the use of other verification tools, such as digital signatures or biometrics. However, the linchpin was authentication through the use of identifying information. Since our last report, authentication has proved successful when properly applied by the commercial community and has been recognized by other experts and by regulators as a necessary tool in the fight against identity theft.

The tragic events of September 11 and the recent reports concerning the use of false identities by some of the hijackers and their cohorts require a reconsideration of whether authentication can be successful when applied to detect and prevent international terrorists committing identity theft.

This report will focus primarily on the type of identity theft that presents the most common threat to commercial entities; the tools, including authentication, that are available to detect and prevent this crime; and an assessment of whether authentication can serve as a tool in combating the new threat of international identity theft.

I. GROWTH OF IDENTITY THEFT

Commentators, law enforcement officials and legislators often too narrowly focus on the effect that identity theft has on the individual victim. Although the harm perpetrated on the individual victim is real and needs to be remedied, by concentrating solely on it, we risk not recognizing the full extent of the problem, and also perhaps not identifying the potential solutions.

In last year's paper we noted that the experience of National Fraud Center, in studying identity theft, supported the following observations:

(1) Identity theft, when committed by the professional criminal, is simply a means to commit a crime.

(2) Identity theft is difficult to track because it is a tool in committing numerous types of crime, including credit card fraud, bank fraud, drug trafficking, etc.

(3) The growth of identity theft appears to be tied to technology, particularly the Internet, and identity theft is becoming an increasing threat to consumer confidence in the Internet as a means to conduct business.

(4) Identity theft, largely as a result of the Internet, is rapidly developing international implications.

There can be no doubt that identity theft has escalated within the past year. The statistics are numbing but nevertheless revealing.

- The Federal Trade Commission, which maintains an identity theft hotline and the Identity Theft Data Clearinghouse, notes that it receives over 1,800 calls per week, as compared to 445 calls per week, when the hotline started in November 1999. The FTC characterizes the growth of identity theft as “dramatic”.⁴
- The FBI estimates that a case of identity theft occurs every two minutes, or roughly 350,000 times per year.⁵
- The Social Security Administration reports that misuse of social security numbers has grown 500% in only four years.⁶
- The Department of Treasury, Financial Crimes Enforcement Network (FinCen) - notes that there were 617 instances of identity theft reported by financial institutions in the period of January through November 2000, as compared to 267 for 1999 and 81 for 1998.⁷
- Estimates of the number of people victimized by identity theft last year range from 500,000 to 700,000.⁸
- The Wall Street Journal estimates that identity theft cost consumers and merchants combined an estimated \$1 billion in the year 2000.⁹

In light of the above statistics, it should come as no great surprise that no one is immune from identity theft. There have been reports of a prosecutor,¹⁰ a legislator,¹¹ a county sheriff,¹² and even the former chairman of the Federal Trade Commission¹³, having been victimized. In one incident alone, involving the so-called “Brooklyn Busboy,” Abraham Abdallah, nearly 200 of America’s most rich and famous people, including Oprah Winfrey, Steven Spielberg and Ted Turner, were reported to have had their identities stolen.¹⁴

II. THE METHODS AND MOTIVES OF IDENTITY THEFT PERPETRATORS

Last year, we observed that the identity theft perpetrator obtains information on his or her victim through three basic approaches; namely (a) through a close personal relationship with the victim, such as a family member or friend; (b) through relatively low-tech means, such as “shoulder surfing,” stealing the victim’s mail or “dumpster diving”; and (c) through sophisticated means, either directly or indirectly, involving the use of the Internet. Undoubtedly, since the Internet presents a means to obtain access to a significantly greater quantity of information, it presents the potential for much greater harm.

The use of the Internet to commit identity theft is increasing. Some of the more notorious examples are described below:

- There were several examples in the past year of “e-mail hoaxes.” These involve either fake Web sites or fake e-mail addresses. They occur through the use of an e-mail transmission when the fraud perpetrator sometimes solicits money, but often simply solicits identifying information. One such example was the “AOL billing scam,” where an e-mail con prompted AOL customers to update personal account information, including credit card and social security numbers.¹⁵ The information, when transmitted by the recipient of the transmission, was diverted to a counterfeit web page. A similar example was the fake FBI Web site, where the fraudster solicited, through an e-mail, information concerning the recipient’s name, address and credit card information, purportedly because it was needed by the FBI.¹⁶
- The West African crime group presented another high-tech means of acquiring information. It presumably hacked into the LifeSource blood donor database where it obtained the personal identifiers of blood donors. Using the identities of 2,000 such donors, the group was accused of having stolen \$2 million worth of airline tickets, hotel reservations, car rentals, computers, and cell phones.¹⁷
- There were several hacking incidents, where personal identifying information was stolen, although no fraudulent transactions were directly tied to them. Some of these examples are the following:
 - The hacking of the University of Washington Medical Center, resulting in the downloading of files from its computer systems containing names, social security numbers, and medical information, on more than 5,000 patients;¹⁸
 - The hacking of Egghead.com that resulted in access to 3.5 million credit cards;¹⁹

- The hacking of CD Universe, an Internet music retailer, by a Russian organized crime group, that resulted in the disclosure of 3,000 credit card numbers.²⁰

Notwithstanding the potential for harm caused by the sophisticated identity thief, most of the reported cases still point to the use of unsophisticated means to obtain the victim's information. Examples are the following:

- The 22 year old Texas waiter, who was charged with using his job at a hotel as an instrument to steal and use the credit card number of a guest;²¹
- The Arlington, Massachusetts mother of two who allegedly slipped into schools in Arlington, Lexington and Somerville and stole credit cards, checks and other personal items from pocketbooks, in empty classrooms, resulting in forgery and credit card fraud of approximately \$75,000.²²
- The employee of the New York State Insurance Fund who was charged with stealing identifying information of state employees to obtain credit and goods in the names of her co-workers. The employee was purportedly part of a large-scale identity theft ring that used the employee's stolen identifying information to steal at least \$100,000 in goods and services.²³
- The fraud group that used employees of California hospitals to steal physicians' medical licenses and other information in order to steal \$1.39 million from the state's Medicaid program.²⁴
- The identity theft ring that operated in 10 states, accused of stealing \$1.2 million in goods and services, through befriending employees of banks and other businesses to get social security and bank account numbers²⁵.

III. IDENTITY THEFT SOLUTIONS

As we noted last year, there are no easy solutions to the identity theft problem. Just as the problem itself is multifaceted, the solution must come from all sectors, government, business and, ultimately, the consumer. Some of the recently proposed solutions are discussed below.

A. International Law Enforcement Cooperation

Recognizing the global impact of all Internet fraud, including identity theft, the United States in late-April joined 12 other countries in an agreement to share cross-border e-commerce complaints.²⁶ Dubbed "econsumer.gov," the purpose of the agreement is to improve international law enforcement agencies' ability to address cross-border Internet fraud.

There are two components to the project. The first is a multilingual public Web site - <http://www.econsumer.gov> - that provides general information about consumer protection in all of the involved countries, contact information for consumer protection authorities in those

countries, and an online complaint form. The information on the Web site is available in English, Spanish, French and German.

The second component of econsumer.gov is a password-protected Web site. This site uses the FTC's Consumer Sentinel network, a database of consumer complaint data and other investigatory information operated by the Federal Trade Commission. Incoming complaints will be shared through the government Web site with participating consumer protection law enforcement agencies that have signed a confidentiality agreement.

B. Linking Governmental Fraud Databases

As we observed last year, identity theft is just one means that a professional fraud uses to accomplish his or her objective, which is to obtain the largest amount of money, as quickly as possible, with the least amount of risk. Although not a case of identity theft *per se*, the Martin Frankel matter is an example of someone who, after being banned for life from the securities industry as a result of fraudulent activities, migrated to the insurance industry where he allegedly stole \$200 million over eight years.

Frankel typifies the pattern of the professional fraud, who will follow the path of least resistance. If the usual path becomes more difficult or presents more risk of detection, the fraud perpetrator will simply migrate to another, presumably easier, path. Since identity theft is simply one tool or path that a professional fraud perpetrator can follow, it is incumbent upon government and industry to make this path as difficult as possible.

Recognizing this migratory pattern of professional frauds, Representative Michael Rogers (R-Mich.) and Representative Michael Oxley (R-Ohio) sponsored H.R. 1408, Financial Services Anti-Fraud Network Act. H.R. 1408 would create a new computer network linking together the existing databases of federal and state banking, securities and insurance regulators in an effort to combat financial fraud. The bill gives regulators six months to plan a network and two years to implement it. The bill recognizes the privacy constraints of such a database and requires that the fraud information be proven before it is inserted into the database.

C. Restricting the Use and Distribution of Personal Identifiers, Particularly Social Security Numbers

There have been at least a half-dozen Congressional bills introduced this year that, in an attempt to combat identity theft, would restrict the use or distribution of personal identifiers, especially social security numbers.²⁷ The aim of each of these bills is to prevent the identity thief from accessing this information.

We believe that although the aim of this legislation is laudable, its effect is potentially devastating. Undoubtedly, some of the incidents of identity theft have been accomplished through the use of an unsavory information broker who, regardless of the purported use, distributes sensitive information to anyone for a fee. However, as illustrated above, the overwhelming evidence is that personally identifiable information that is used for identity fraud is not obtained through an information broker. It is obtained by the identity thief who either obtains the information from a known victim, steals the information in a conventional

manner or uses a high-tech hacking method. In the interest of protecting their anonymity, identity thieves rarely use information brokers, however unsavory, that are not part of their conspiratorial ring.

This is not to say that personally identifiable information should be disseminated to the general public. It should not. However, to believe that legislating social security numbers “back into their bottle” will have a meaningful effect on identity theft is over-simplistic and potentially counterproductive. In fact, it has significant unintended consequences impacting financial practices and risk management.

D. Authentication as a Solution

Last year, we proposed that the approach that has the greatest potential for successfully altering the identity fraudster’s path is authentication. This is the process by which a credit grantor determines that the consumer is who he or she says they are. Over the past year, this process has proved successful where properly applied and it has been promoted by governmental regulators.

(1) Verification Techniques

There are three primary means of verifying the identity of an individual. They are: (a) a signature document, such as a passport or driver’s license, or the electronic equivalent, a digital certificate or signature; (b) biometrics; and (c) authentication, or the use of information unique to the individual, for example passwords, PINS or discrete identifying information, such as names, social security numbers and addresses.

A digital signature is a process used in electronic transmissions to verify to the person receiving the information through an electronic transmission (“the receiver”) that the person sending the information (“the transmitter”) is who he or she purports to be and that the message has not changed from the time it was transmitted. How a digital signature works requires an understanding of cryptography and public key infrastructure. However, basically, the signature is contained in an encrypted segment of software, known as a digital certificate, and it is interpreted by the security features in a Web browser program to authenticate the transmitter. Third parties have evolved that issue digital certificates. These certificate authorities issue the digital certificates to subscribers, binding their identities to the key pairs used for the digital signature process.

There are various levels of security used to protect the identities of the certificate owners. However, the known security limitation of the system is the process utilized to determine the person obtaining the digital signature and certificate is truly that person. The only known means of making this determination is through the process of authentication.

Biometrics is the use of a body part as a signature to verify the person. The most common means of biometrics involve fingerprinting, facial recognition and eye retina scanning. Biometrics has been suggested primarily for the in-person transaction and it is intended to perform the same verification function in that environment as the digital certificate does in the e-commerce environment. Its limitation, however, is the same as the digital

certificate. It is dependent on authentication to verify, in the initial instance, that the person exhibiting a particular set of fingerprints, facial characteristics or eye retina is truly the person whose identity is provided.

The authentication process utilizes independent business and/or consumer data to verify the person or business entity with whom the company is doing business. This methodology allows for verification not only in the in-person transaction, but also in the "faceless" Internet transaction.

The required degree of authentication varies. It depends on the extent of the appreciation exhibited by the fraud perpetrator of the risk involved in using identity theft in a particular industry, at a particular point in time. For example, what may be required to authenticate a person applying for a cellular account may differ from the authentication required of a person opening a checking account at a bank. Nevertheless, regardless of the degree of authentication required, authentication is dependent on the ability of the credit grantor, commercial establishment or governmental entity to obtain personal and business related information in order to independently verify the individual.

The authentication process need not be time consuming or difficult for the consumer to experience. This factor is often referred to as the insult rate. Studies have shown that if the insult rate is too high, the consumer will go somewhere else or will use a different medium to complete the transaction. Authentication can be made to appear seamless, thereby meeting the insult rate objective. For authentication to work, it is essential that the credit grantor, commercial establishment or governmental entity have access to the appropriate types of identifying data necessary to implement an authentication process. This means that private industry must have the right, and the means, to obtain the identifying data needed to independently verify the individual. There is, of course, a corresponding obligation on the part of credit grantors, commercial establishments and governmental entities to recognize their responsibility concerning the use of this data. They must responsibly maintain the data and use it in accordance with the purpose for which it was provided.

Finally, some of the verification techniques are dependent on the medium in which the transaction occurs. For example, although a properly documented passport or verified fingerprint might be preferable in an in person transaction, they are useless in a telephone or e-commerce transaction. Similarly, although a PIN or password might be preferable for an existing account, they do not apply in an account opening transaction. For the latter transaction, particularly when conducted by phone or electronically, reliance must be placed on personal identifiers, which can be examined in logical sequence to determine the identity of the individual.

(2) Governmental References to Authentication Techniques

The Office of the Comptroller of the Currency (OCC), in an April 30 Advisory Letter,²⁸ recognized the authentication process as an appropriate means for banks to combat identity theft in the process of opening a new account. With regard to verifying identities when a bank is opening an account, the OCC stated as follows:

To reduce the risk of fraudulent applications, banks should establish verification procedures to ensure the accuracy and veracity of application information. In conjunction with their existing account opening procedures, banks should consider how best to independently verify information provided on account applications to detect incidents of identity theft. Verification of personal information may be accomplished in a number of ways. Some alternatives to consider include: (a) *positive verification* to ensure material information provided by an applicant is accurate; (b) *logical verification*; and (c) *negative verification* to ensure information provided has not previously been associated with fraudulent activity. (Footnote omitted.)

By “*positive verification*”, the OCC explained that it meant, “[c]onsulting third party sources to assess the veracity of information submitted to a consumer.” Although there were several different ways suggested by the OCC to obtain positive verification, certainly the use of existing databases would be an appropriate means to accomplish this objective. “*Logical verification*,” according to the OCC means, “[a]ssessing the consistency of information presented in an application.” The OCC explained that a bank could verify if the zip code and telephone area code provided on the application covered the same geographical area. The OCC specifically referred to products that are currently available that managed this task. Finally, “*negative verification*” according to the OCC, means “[e]nsuring that information provided on an application has not previously been associated with fraudulent activity.” Although the OCC did not provide a means to obtain the negative verification, fraud alerts and other warning systems exist for identifying known fraudulent transactions.

The Federal Financial Institution Examination Council (FFIEC)²⁹ issued a similar guidance with regard to the use of positive, logical and negative verification, in an account origination transaction, for electronic banking.³⁰ Specifically with regard to “*positive verification*,” the FFIEC recommended reliance on a “trusted database,” as a source of information to compare an applicant’s answers to a series of detailed questions.

Finally, PricewaterhouseCoopers’ Scott Charney, in testimony before a House Subcommittee,³¹ emphasized that in order to protect consumers, merchants must be better at authenticating their business and consumer customers. Although he used different terminology, Charney essentially endorsed the verification techniques described in this paper. Specifically with regard to what we characterize as “authentication,” Charney stated, “Recognizing the impracticability of authenticating electronic and telephonic transactions using biometrics and possessions, merchants have relied upon the third type of authentication: “something the buyer knows,” often referred to as a “shared secret.” In this context, Charney noted, “More commonly both merchants and consumers rely upon a third party to verify the secret. For example, if a consumer is purchasing goods with a credit card, he may also be asked

to provide his home address as a shared secret; this is information that the merchant can have verified by a third party (e.g., a credit reporting agency).”

(3) Successful Application of Authentication Techniques

National Fraud Center and its affiliated companies have witnessed firsthand the benefit of authentication tools used in the proper context. Bank credit card and commercial entities that have used authorization tools have confirmed their effectiveness.

IV. AUTHENTICATION AS A POTENTIAL SOLUTION TO INTERNATIONAL IDENTITY THEFT

Although the reports on the individuals involved in the September 11 events provide only sketchy details, they have confirmed that at least four of the hijackers used false identities when boarding the planes.³² The hijackers apparently supported their claimed identities with phony passports, drivers' licenses and other documents. The identities they assumed were of real people who live in Saudi Arabia and Tunisia.

Whether the use of authentication techniques by government entities or airline ticket agencies could have detected the terrorists who used the false identities is not yet known. However, what we do know is that international terrorists present the same problems, with regard to confirming identities, as do any other international criminals. What Middle Eastern terrorists have in common with South American drug traffickers and West African and Eastern European fraud rings, in addition to the fact that they are all organized international criminals, is that the identities they assume are most often of people in their native countries or of that immediate area. Unfortunately, most of the authentication products that exist today are comprised of domestic data, not data on foreign nationals.

The difficulty in detecting the international identity thief is due to the paucity of data that is presently available, either commercially or to the government, that can help detect whether fraudulent identifying information is being used. Absent the availability of this data, confirmation of identity is extremely difficult.

Much has been stated concerning the potential benefit of using some form of biometrics in confirming identification of the international identity thief. However, a biometrics technique is only as good as the data available. For example, computerized face recognition tools are successful only if the individual's face is in the computer database. Since these databases are usually limited to convicted felons or a similar group of miscreants, the identity thief who is not yet known as a criminal will not be detected.

On the bright side, there is some data that, if made available, we believe can have a significant effect in detecting the use of false identity by international criminals. Some of this data is the following:

- Social security numbers, and related information, from the Social Security Administration database;
- United States and international passport data;

- International criminal and fraud databases;
- International and domestic sanctions data; and
- Drivers' license data from all fifty states.

This data is generally unavailable because of various privacy concerns. However, in order to combat international identity theft, we need to explore all options and, if the data described above can be used in a restricted and regulated manner, it is a viable option in an authentication process.

V. CONCLUSION

The observations we made last March concerning identity theft continue to be valid today. Identity theft, when committed by a professional criminal, is simply a tool, a means to an end. Consequently, when an arrest is made, identity theft is considered by law enforcement as a lesser offense included in the more serious offenses of bank fraud, securities fraud, drug trafficking, etc. Therefore, tracking it is difficult, and obtaining intelligence information on how the crime is committed remains a challenge.

Technology continues to foster identity theft primarily, although not exclusively, fueled by the Internet. With the Internet, the global implications of identity theft continue to confound law enforcement, policy makers and merchants.

What is more apparent today than last year is that identity theft is becoming more of a tool for the international crime groups. The fraud rings, drug cartels and even the terrorists are using it to achieve their broader criminal aims. Further, it is no longer valid to simply view it as a tool to commit fraud. It is a tool to gain access to physical locations, such as airplanes, federal buildings and other restricted areas. It can also be a tool to gain access to computer systems.

We no longer have the luxury to deal with the identity theft problem with the velvet gloves of privacy sensitivities. We need to explore all possible solutions. Authentication, in our opinion, can be successfully applied to this new global threat.

We recognize that we can not compromise our fundamental rights and freedoms in the process, but we must also recognize that it is our fundamental rights and freedoms that may be hanging in the balance.

¹ Mr. Willox is the Chairman of National Fraud Center, Inc. and Chief Officer for Privacy, Industry and Regulatory Affairs for the LexisNexis Group, a division of Reed Elsevier, plc. National Fraud Center, Inc. is a member of LexisNexis.

² Mr. Regan is a member of the law firm of Cozen O'Connor. He is Chairman of the firm's Privacy Law and Regulation Department. Mr. Regan also practices in the firm's Fraud Practice Group.

³ Willox, Norman A. Jr., "Identity Theft: Authentication As a Resolution," (www.nationalfraud.com/identity%20theft%203.13.htm)

⁴ Federal Trade Commission, “Information on Identity Theft for Consumers and Victims From November 1999 Through June 2001.” www.consumer.gov/idtheft/reports/01-06r.pdf.

^{5,8} Statement of Sen. Dianne Feinstein (D-Calif.), introducing S1055, Privacy Act of 2001, June 14, 2001.

⁷ Department of the Treasury, Financial Crimes Enforcement Network, “The SAR Activity Review,” June, 2001, at pp.14-15, www.ustreas.gov/fincen/sarreview2issue4web.pdf

⁸ “The Growing Global Threat of Economic and Cyber Crime,” The National Fraud Center, Inc. in conjunction with The Economic Crime Institute, Utica College, December, 2000.

⁹ Greenberger, Robert S. and Simpson, Glenn R., “Identity Theft Dogs Credit Bureaus In the Supreme Court and Congress,” The Wall Street Journal, April 12, 2001.

¹⁰ Feinstein, Dianne, “We Need Additional Privacy Laws Now,” InformationWeek, August 20, 2001.

¹¹ Braden, Tyra, The Morning Call, FraudInfo Newsletter, August 22, 2001.

¹² Bergquist, Lee, “Identities Under Fire In Widespread Thefts,” Milwaukee Journal Sentinel, August 19, 2001.

¹³ Remarks of Robert Pitofsky at the Identity Theft Summit, March 15, 2000.

¹⁴ Greenberger, Robert S. and Simpson, Glenn R., “Identity Theft Dogs Credit Bureaus In the Supreme Court in Congress,” The Wall Street Journal, April 12, 2001.

¹⁵ Bridges, Tony, “Identity Theft By Way of AOL,” Knight Ridder News Service, July 19, 2001.

¹⁶ “Fraud: Are You Sure That’s An FBI E-Mail?” National Journal’s Technology Daily, July 17, 2001.

¹⁷ Kazak, David R., “Seven Accused of Stealing Identities For Credit Cards,” Herald Legal Affairs, July 16, 2001.

¹⁸ Cox, Paul, “Social Security Numbers Play Big Role In Web Identity Theft,” The Wall Street Journal, July 16, 2001.

^{19,22} Bergquist, Lee, “Identities Under Fire In Widespread Thefts,” Milwaukee Journal Sentinel, August 19, 2001.

²¹ Boyd, Deanna, “Waiter Accused of Credit Card Number Theft,” The Fort Worth Star-Telegram, July 27, 2001.

²² Martinez, Jose, "Arlington Mom Avoids Jail Time For Identity Theft," The Boston Herald, July 28, 2001.

²³ "New York Charges Insurance Fund Employee With Identity Theft," Consumer Financial Services Law Report, August 20, 2001.

²⁴ Rose, Joan R., "Doctors and Patients Both Fall Victim To Identity Theft," Medical Economics, September 18, 2000.

²⁵ Bergquist, Lee, "Identities Under Fire In Widespread Thefts," The Milwaukee Journal Sentinel, August 19, 2001.

²⁶ "Challenges Posed By Cross-Border Fraud On Internet Leads To International Effort," Electronic Commerce and Law Report, May 2, 2001.

²⁷ S.324, Social Security Number Privacy Act of 2001; S.1014, Social Security Number Privacy and Identity Theft Prevention Act of 2001; S.1055, Privacy Act of 2001; S.1399, Identity Theft Prevention Act of 2001; H.R. 2036, Social Security Number Privacy and Identity Theft Prevention Act of 2001; H.R. 2135, Consumer Privacy Protection Act; H.R. 2720, Consumer's Right to Financial Privacy Act.

²⁸ OCC Advisory Letter 2001-4 (Identity Theft and Pretext Calling)

²⁹ The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC) the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.

³⁰ FFIEC Guidance, "Authentication in an Electronic Banking Environment," August 8, 2001 (www.ffiec.gov/pdf/pr080801.pdf).

³¹ House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, Hearing Re: "On-line Fraud and Crime: Are Consumers Safe?" Prepared Witness Testimony of Scott Charney, May 23, 2001.

³² Bulkeley, William M., "Hijackers' Deeds Highlight Issue of Rampant Fake ID's In The U.S.," The Wall Street Journal, September 26, 2001; "New Terror Probe Suspect Arrested, But Doubts Grow Over Hijackers' Identities," Yahoo!News, September 21, 2001.