



## **IDENTITY FRAUD: PROVIDING A SOLUTION**

*BY: NORMAN A. WILLOX, JR., and THOMAS M. REGAN, ESQ.*

### **ABOUT THE AUTHORS**

Mr. Willox is the Chairman of National Fraud Center, Inc. and Chief Officer for Privacy, Industry and Regulatory Affairs for the Lexis-Nexis Group, a division of Reed Elsevier, Inc. Mr. Willox is an expert on identity fraud prevention and investigation, having devoted most of his professional career to studying, and devising solutions for, this multifaceted problem.

Mr. Regan is a member of the law firm of Cozen O'Connor, and Chairman of the Privacy Law & Regulation Department. He is a former prosecutor and has litigated many cases involving commercial fraud matters.

The authors were assisted in the preparation of this paper by Matthew F. Henry, Esq. Mr. Henry is a 2001 graduate of Villanova Law School and is an associate with Cozen O'Connor. He has demonstrated a particular aptitude for understanding the identity fraud problem.

This paper is the third in a series of articles that Mr. Willox and Mr. Regan have collaborated on. The first, "Identity Theft: Authentication As A Solution," ([www.nationalfraud.com/IDENTITY%20THEFT%203.13.htm](http://www.nationalfraud.com/IDENTITY%20THEFT%203.13.htm)) was submitted at the National Identity Theft Summit, convened by the United States Department of the Treasury, in conjunction with the Federal Trade Commission and other federal agencies in March 2000. The second article, entitled "Identity Theft: Authentication As A Solution – Revisited," ([www.lexisnexis.com/aoa](http://www.lexisnexis.com/aoa)) was released in October 2001.

### **EXECUTIVE SUMMARY**

It is now widely accepted that the terrorist attacks of September 11, 2001 were orchestrated by a well-financed, highly motivated and resourceful terrorist gang. Differing only in their motivation, this terrorist criminal enterprise can be favorably compared to other global criminal cartels, emanating from the far reaches of the world. Among other attributes, these global criminal enterprises rely upon little known, non-descript individuals to perpetrate the crimes. Taking advantage of ineffective, or non-existent, identification systems, these individuals manage to mask who they are, where they live and where they have been.

Prior to September 11, governments and businesses were sensitive to identity imposters, but they viewed the problem as primarily a financial matter, that is, as a significant component of fraud. Called identity theft, statistics were gathered about its effect on businesses; hearings were conducted on its harm to individual victims and, in 1998, federal legislation was passed to criminalize it.

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 identification 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 identity 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.”

The White Paper proposes a solution to one important aspect of the identity fraud problem and a process for arriving at a solution for the balance of the problem. Recognizing that the science of human identification provides three basic means of identification; namely, knowledge-based, biometrics and tokens, the White Paper acknowledges that an identity fraud solution, depending on the environment in which it is being applied, could utilize all three means.

However, there is one very important phase in the identity verification process, when, regardless of the environment, only a knowledge-based solution can be used. This phase is the beginning of the identity verification process when the individual is new to the verifier. It is when the verifier has had no previous contact with the individual. It is this stage of the identity verification process that is most susceptible to abuse. Because biometrics and token solutions are not available at this phase of the identification process, there can only be a knowledge-based solution.

This White Paper proposes a particular knowledge-based solution for the beginning phase of the identity verification process. Referred to as “authentication,” the solution is based on the verifier possessing certain information pertaining to the individual, from which the verifier can confirm the identity of the individual. The authentication solution is aided by a statistically-based model which can score the verification of the person’s identity. The model uses certain identifying information, pertaining to an individual, that is time sensitive. Examples of the types of information that can be used are an individual’s present address and phone number, as well as past addresses and phone numbers which the individual had at certain points in time. The logic of the model is predicated on the theory that an imposter may know some of the information pertaining to a real individual, but he or she will likely not know all of the real person’s identifying information that is critical to the model.

This knowledge-based solution has proved successful in commercial identification environments. The White Paper observes that, assuming the availability of the critical identifying information, the knowledge-based system can be applied in any identification environment, regardless of the presence of the individual, anywhere in the world.

Beyond the beginning phase of the identity verification process, the White Paper proposes creating a task force to determine the appropriate means of identification, which will be dependent on the environment in which the identification takes place. It is recommended that the members of the task force be drawn from all of the interested groups, both public and private, and that it be administered by the Federal Government. The White Paper identifies the factors that bear on the identification process and recommends that the task force consider these factors on arriving at proposed solutions.

## **I. INTRODUCTION**

On September 11, 2001, 19 terrorists hijacked four jet airliners, crashing two of them into the World Trade Center Towers, one into the Pentagon and a fourth into a field in western Pennsylvania.<sup>1</sup> Two of the terrorists were Abdul Azziz Alomari and Ahmed Saleh Alghamdi.<sup>2</sup>

Alomari was in a group of five terrorists who hijacked American Airlines Flight 11, bound from Boston to Los Angeles, which ultimately crashed into the north tower of the World Trade Center in New York City.<sup>3</sup> Alghamdi was in another group of five terrorists who hijacked United Airlines Flight 175, bound from Boston to Los Angeles, which ultimately crashed into the south tower of the World Trade Center in New York City.<sup>4</sup> In addition to the obvious acts of terrorism, Alomari and Alghamdi were guilty of identity fraud.

About a month before the hijackings, Alomari and Alghamdi used an accomplice to approach a secretary of a Virginia lawyer.<sup>5</sup> They paid her to complete false Virginia identity affidavits and residency certifications.<sup>6</sup> The documents indicated that Alomari and Alghamdi had Virginia residences, when, in fact, they resided in Maryland motels.<sup>7</sup> Using the false documents, notarized by the Virginia secretary, Alomari and Alghamdi obtained Virginia state identification documents.<sup>8</sup> These identification documents were used by Alomari and Alghamdi on September 11 to board the ill-fated planes.<sup>9</sup>

Reports are replete that the terrorists responsible for the September 11 hijackings made wholesale use of false identities, fraudulent identification documents and fictitious social security numbers.<sup>10</sup> Purportedly, five of the terrorists, in addition to Alomari and Alghamdi, procured fraudulent Virginia identification cards.<sup>11</sup> Another five reportedly obtained fake social security numbers.<sup>12</sup> Authorities believe that, at one time or another, each of the 19 terrorists may have used false social security numbers.<sup>13</sup>

Identity fraud, that is, the criminal use of false identities or fraudulent identification documents, has been the subject of much discussion, debate and legislation during the recent past. However, most of that attention has been in the context of its use as an instrument of fraud, such as in credit card fraud, securities fraud, and bank fraud. The activities of the September 11 terrorists now cause us to realize that identity fraud is not just the tool of the con artist. It is, when properly recognized, indigenous to any criminal enterprise, whether it be drug trafficking, alien smuggling or cyber stalking.

## **II. REDEFINING THE IDENTITY FRAUD PROBLEM**

On October 30, 1998, following considerable debate about the deleterious effects of identity theft, the Federal government passed the Identity Theft and Assumption Deterrence Act of 1998 (ITADA).<sup>14</sup> It cast as an identity thief anyone who “[k]nowingly 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.”<sup>15</sup> State governments have also prohibited identity theft, using a definition of identity thief that is substantially similar to that found in ITADA.

Identity theft, as prohibited in ITADA and the state equivalents, is limited to the use of the “[m]eans of identification of another person” (emphasis supplied).<sup>16</sup> This focus on the use of

a real person's identifiers, is sometimes referred to as "true person fraud."<sup>17</sup> The term has its origins in the harm that the statute intends to proscribe, that is, to an existing person, whose identity is assumed by the identity thief.<sup>18</sup>

Identity theft, as the legislative history to ITADA amply demonstrates, is a serious problem. According to the United States Secret Service, of the approximate 10,000 financial crime arrests that its agents made during 1997, 94% involved identity theft.<sup>19</sup> The United States Postal Inspectors and the Secret Service have reported that organized criminal elements are using identity theft as part of their international enterprises, involving not only financial crimes, but also drug-related, immigration and violent crimes.<sup>20</sup> The ITADA legislative history further documents the effect of identity theft to individuals and corporate victims. Master Card estimated that of its approximate \$407,000,000 in fraud losses in 1997, 96% of it was attributed to identity theft.<sup>21</sup> The Secret Service estimated that in 1997 the losses caused by identity theft, for which it made arrests, amounted to \$745,000,000, with the losses doubling from the previous two years.<sup>22</sup>

As daunting as the above identity theft statistics are, the fact is that they are only the tip of the iceberg. When we consider that the collective losses occasioned by credit card fraud, insurance fraud and health fraud are in the hundreds of billions of dollars per year, and that identity theft comprises a significant part of these crimes, we can conservatively estimate that identity theft accounts for at least tens of billions of dollars in losses.<sup>23</sup>

Identity theft has, indeed, shook our national consciousness. However, as devastating its harm, the scope of the identity theft problem does not capture the terrorists' use of false identities and false identification documents. Alomari and Alghamdi did not assume an existing person's identity. In fact, they continued to use their own names, albeit with false addresses supported by fraudulently obtained identification documents. To address this problem, from a prevention

standpoint, requires that we consider not only identity theft true person fraud, but any criminal use of false identifiers or false identification documents.

Some of the recent accounts of the use of false identifications and false identification documents illustrate the extent of this problem. In Tuscaloosa, Alabama, an employee in the county license office was arrested and charged with selling or giving away outdated drivers' licenses.<sup>24</sup> According to Alabama Bureau of Investigation Lieutenant Mike Manlief, five to ten of the outdated licenses were given or sold to people under the age of twenty-one, so that they would be able to purchase alcohol.<sup>25</sup> In Elgin, Illinois, Sergeant Brad Entler of the police department observed that fraudulent ID cases are "a total epidemic."<sup>26</sup> He expressed particular concern about gang member use of false identifications to purchase guns.<sup>27</sup> In Portland, Oregon, a raid of a suspected identity theft ring resulted in the seizure of powerful explosives, methamphetamines, stolen mail and fake drivers' licenses.<sup>28</sup>

The term "identity theft," with its connotation of true person fraud, is too narrow a concept to capture these diverse uses of false identities and false identification documents. We must use a term that properly reflects the broader problem. Although "identity fraud" has been sometimes used interchangeably with "identity theft," we submit that, when properly used, "identity fraud" envelops the entire breadth of the problem.

Identity fraud is certainly a financial fraud problem. It is, as the Secret Service reports, a substantial part of the financial crimes that the Secret Service investigates, including bank fraud, computer and telecommunications fraud, access device fraud, advanced fee fraud, etc.<sup>29</sup> Law enforcement officials also identify social program fraud, tax refund fraud and mail fraud as containing intrinsic elements of identity fraud.<sup>30</sup> In fact, identity fraud permeates as many as twenty-five different financial fraud crimes.<sup>31</sup> However, identity fraud is more than just a financial fraud problem.

Identity fraud is certainly a terrorism and illegal immigration problem. Alomari and Alghamdi, and their co-terrorists, illustrate the use of identity fraud in committing acts of terror. Terrorists, though, do not limit their criminal activities to creating mayhem. As Dennis Lormel, Chief of the FBI's Financial Crimes Section, told the House Committee on Financial Affairs, last October, "[t]errorist cells often resort to traditional fraud schemes to fund the terrorists' activities."<sup>32</sup> Lormel included identity theft as one of the terrorists' "prevalent" fraud schemes.<sup>33</sup> He noted, "The ease with which these individuals can obtain false identification or assume the identity of someone else, and then open bank accounts and obtain credit cards, make these attractive ways to generate funds."<sup>34</sup> However, as serious a component of terrorism identity fraud is, identity fraud is not solely a terrorism problem.

As the Postal Inspectors have reported, identity fraud is a drug trafficking problem.<sup>35</sup> It is also a cyber crime problem, as Web stalkers hide behind the Internet's anonymity.<sup>36</sup> It is a computer hacking problem, as Eastern European criminals assume or make up passwords and user IDs to steal sensitive consumer data, in order to extort unsuspecting companies.<sup>37</sup> It is an alien smuggling problem, a gun-running problem and a money-laundering problem. It is, as law enforcement officials have confirmed, a problem at the core of many different types of organized crime, committed locally, nationally and globally.<sup>38</sup>

### **III. IDENTITY FRAUD SOLUTIONS – A METHODOLOGY**

Since September 11, the country's focus has been in preventing terrorism, including the terrorists' use of identity fraud. Congressional hearings have been conducted; reports have been submitted; and the popular press has frequently provided commentary, on potential solutions. The fact is that, notwithstanding the lengthy discussions that have transpired, the country has yet to identify any particular solution to the identity fraud problem that has universal application in preventing terrorism.

Admittedly, we have witnessed a virtual cornucopia of proposed solutions to the identity fraud problem in the terrorism context, from biometrics to national identification cards. Promoters of biometrics point to the history of law enforcement use of fingerprint science;<sup>39</sup> the use of facial recognition at last year's Super Bowl which was attended by some 60,000 people;<sup>40</sup> and the availability of hand geometry biometrics which have reportedly been successfully deployed since 1985 at airports, nuclear facilities, chemical plants and other facilities constituting the nation's critical infrastructure.<sup>41</sup> Proponents of national identification, including the prominent civil libertarian, Professor Alan Dershowitz, support it primarily because they believe it is simply needed in this age of terrorism, as our existing means of identification, such as drivers' licenses, have proved ineffective.<sup>42</sup>

Detractors of biometrics point to, among other things, the cost of installation, absence of proof of effectiveness and, most importantly, their potential use as a means to aggregate personal information such as spending habits, medical treatment, etc.<sup>43</sup> National identifications are often criticized for substantially the same reasons. Katie Corrigan, legislative counsel on privacy for the ACLU, in testimony before a House committee, captured the privacy objection by stating, "Unlike workers in Nazi Germany, Soviet Russia, Apartheid South Africa and Castro's Cuba, no American faces the demand, 'Papers, please.'"<sup>44</sup>

The mutual force of the arguments on either side of the biometrics and national identification issues has evolved into a virtual equipoise. We know we need solutions, but we fear the results. Fundamentally, what is lacking is a framework, a rudder, to guide us to the appropriate solutions and, ultimately, we need facts, not suppositions, to resolve the inevitable tests.

UCLA Law Professor Lynn LoPucki provides a framework, in his discussion of "the currently prevailing theory of human identification."<sup>45</sup> Citing Professor Roger Clarke's

“foundational article”<sup>46</sup> where Clarke defined human identification as “the association of data with a particular human being,”<sup>47</sup> LoPucki provides three basic means for making identifications. The first such means is “knowledge-based” where persons are “[r]ecognized by demonstrating that they are in possession of information which only that person would be expected to know.”<sup>48</sup> The second basic means of human identification, according to LoPucki, is “token-based” identification, where a person is recognized by their possession of an item, such as a national identity card, or a driver’s license, or a passport.<sup>49</sup> Each of these “tokens” bears a description of the person that presumably would not match an imposter’s person. The third means of human identification is “biometrics” which LoPucki states, quoting Clarke, refers to “a variety of identification techniques which are based on some physical and difficult-to-alienate characteristics.”<sup>50</sup> All three means of identification should be considered when devising an identity verification solution. However, in certain identification environments, not all of the means of identification may be necessary, or even appropriate.

Undoubtedly, the most difficult identification environment is where the individual who is seeking identity verification is unknown to the verifier, and has not been previously verified. This initial phase of identity verification can only occur through a knowledge-based, authentication<sup>51</sup> solution. As indicated above, there has been much discussion about implementing an effective token, or biometric, based system, such as a national identification card or a more narrowly applied “trusted-traveler” card, which is presently being considered by the United States Department of Transportation for airline passengers.<sup>52</sup> However, no such systems presently exist and, even if they did, there would still be a need for an initial authentication process founded in a knowledge-based solution. To utilize a biometric or token based system, without first authenticating an individual, simply provides an opportunity for an imposter to link a false name, or other false identifiers, with the imposter’s biometrics or token.

There have been attempts in the past to use a knowledge-based system of identification, limited to discrete identifying information, such as a person's social security number, or a mother's maiden name. These systems have failed when the social security number or the mother's maiden name became widely circulated, leaving them accessible by identity thieves. However, successful applications have been made of knowledge-based identifiers, when a sufficient number of them are combined so that they can be statistically confirmed through the use of models and scores.

A successful knowledge-based authentication solution is dependent upon the ability of the verifier to possess a sufficient quantity of information pertaining to individuals, from which the verifier can determine whether a subject person is who he or she says they are. The underlying basis for this solution is that only the real "John Doe" would know all of the identifying information to be able to match the control data possessed by the verifier. The matching process should be capable of objectively scoring the information provided, so that the potential absence of certain information does not necessarily result in the inability to authenticate a particular person.

This type of knowledge-based authentication solution is not novel. It has been used successfully in the financial community.<sup>53</sup> It has been demonstrated there that the information that is particularly significant is that which relates to an individual at a particular point in time. Examples of this type of time-sensitive information are current and past addresses and phone numbers, both residential and business. Additional examples of time-sensitive information are Internet IP addresses and certain types of meaningful occurrences in a person's life, such as dates of birth, marriage and even death, as an imposter may not realize that the identity that he or she is using is of a person who has died.

Knowledge-based authentication, predicated upon the verifier possessing identifying information, would be directly responsive to the verification procedures contemplated by Congress in the USA PATRIOT Act.<sup>54</sup> The Act, at § 326, “Verification of Identification,” requires the Secretary of the Treasury to prescribe regulations for financial institutions to verify the identities of customers. Specifically aimed at combating money laundering, Section 326 prescribes that the verification regulations, must, as a minimum requirement, require that financial institutions maintain records “[o]f the information used to verify a person’s identity, including name, address, and other verifying information . . .”<sup>55</sup>

In fact, we submit that the knowledge-based authentication solution proposed will be responsive in any authentication environment, domestically, internationally and electronically. The prerequisite is to gather sufficient control data so that a mathematical model can statistically verify the identity of an individual. The challenge, particularly in an international setting, is to secure the requisite verifying information.

In implementing a knowledge-based authentication solution, there are certain non-identification factors, driven by the identification environment, that must be considered. The first such factor is the time to conduct the identification process. For example, in an instant credit-granting environment, the credit applicant will not wait more than several minutes for the verification process to be completed. This time period, sometimes referred to as the “insult rate,” may be significantly less in one identification environment than it is in another. For example, in an electronic transaction, the insult rate can be measured in seconds. Invariably, there is an applicable insult rate, whether the process is foreign visa issuance, airplane travel or daycare employee applications.

Another significant non-identification factor to consider for any proposed solution is the intricacy of integration. For any solution to be successful, it must be cost effective. Ideally, the

solution should be compatible with existing systems and it must be capable of being applied by existing staff. However, if the solution is not readily compatible with existing resources, the cost of application must be balanced against the particular need for positive identification.

The characteristics of the criminal committing identity fraud must also be taken into consideration. Since the criminal in an organized enterprise can possess significant intelligence, resourcefulness, adaptability and mobility, the contemplated solution must account for these traits. It must be a process that is not easily discernable, can be changed quickly and often and it must account for the international criminal, who knows no boundaries and respects no borders.

In summary, any proposed solution must meet established standards in proving that it can work effectively in a particular identification environment and respond appropriately to the characteristics of the prospective identity fraud. Such standards or tests will inevitably change from environment to environment, depending on the level of risk involved.

These tests, or studies, need to be conducted quickly, efficiently, and fairly. Because of the broad scope of the identity fraud problem, the studies should be supervised by the federal government, and conducted by a task force comprised of all interested parties in both the public and private sectors. The task force should consider all of the factors bearing upon the identity fraud problem and the prospective solutions, including the following:

- (1.) All critical identification environments, including passport and visa issuance; drivers' license issuance; birth and death certificates; etc.
- (2.) The effectiveness of all proposed solutions for particular identification environments;
- (3.) The established ability of the solutions to satisfy the factors of time and integration;
- (4.) The characteristics of the identity fraud criminal, including his resources, adaptability and global mobility;

- (5.) The cost of implementation of any such solution, using a cost benefit means of analysis; and
- (6.) The social impact of any solution, including its effect on the privacy of individuals.

#### IV. CONCLUSION

Identity theft, the taking of a person's identity for the purpose of committing a criminal act, is a serious concern as it violates the individual victim and wreaks huge financial losses on the commercial victim. However, the crime of using false identifiers and false identification documents transcends identity theft, as it includes not only the identity thief, but also the drug trafficker, the alien smuggler and the terrorist. One who commits this crime of identity fraud needs to be culled out and prevented through new, innovative and effective solutions.

Borrowing from the academic science of human identification, we have provided a framework for devising appropriate solutions. These solutions, we submit, can only be derived through the earnest efforts of all interested parties, through a task force organized under the auspices of the federal government.

---

<sup>1</sup> United States v. Zacarias Moussaoui, U.S.D.C., E.D. Va., Dec. 2001 term, Indictment, Paragraphs 104-107.

<sup>2</sup> Id. Paragraphs 104-105.

<sup>3</sup> Id. Paragraph 104.

<sup>4</sup> Id. Paragraph 105.

<sup>5</sup> United States v. Kenys A. Galicia, U.S.D.C. E.D. Va., Oct. 2001 term, Indictment, Paragraphs 7,8.

<sup>6</sup> Id. Paragraphs 7,8.

<sup>7</sup> Krim, Jonathan and O'Harrow, Robert Jr., "National ID Cards Gaining Support," Washington Post, December 17, 2001.

<sup>8</sup> See Galicia Indictment, supra, note 5, paragraph 9.

<sup>9</sup> See Krim article, supra, note 7.

<sup>10</sup> Id. See also, Bulkeley, William M., "Hijackers Deeds Highlight Issue of Rampant Fake Ids in the U.S.," Wall Street Journal, September 26, 2001; "Asset Freezes Against Terrorism Has Weak Track Records," Dow Jones Newswires, September 26, 2001; "New Terror Probe Suspect Arrested, But Doubts Grow Over Hijackers Identities," AFP, September 21, 2001; Shaw, E. Clay Jr., prepared remarks before the Committee on Ways and Means, Subcommittee on Social

---

Security and Committee on Financial Services Subcommittee on Oversight and Investigations, hearing on “Preventing Identity Theft by Terrorists and Criminals,” November 8, 2001, p. 1; Kelly, Sue W., prepared remarks before the Committee on Ways and Means, Subcommittee on Social Security and Committee on Financial Services Subcommittee on Oversight and Investigations, hearing on “Preventing Identity Theft by Terrorists and Criminals,” November 8, 2001, p. 1.

<sup>11</sup> See Krim article, *supra*, note 7.

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> Identity Theft and Assumption Deterrence Act, Public Law 105-318, 112 STAT. 3010, October 30, 1998, codified at 18 U.S.C. § 1028 (1999).

<sup>15</sup> 18 U.S.C. § 1028(a)(7).

<sup>16</sup> *Id.*

<sup>17</sup> General Accounting Office, “Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited,” May, 1998, p. 41 (GAO/GCD-98-100BR) (stating that a Trans Union official categorizes an incident where someone assumes a “true” identity as “true person fraud”).

<sup>18</sup> Identity Theft and Assumption Deterrence Act, S. Rep. No. 105-274, at 6 (1998) (noting that the Federal Trade Commission testified that the identity theft victims “suffer real harm” with the effect of the theft being “significant and long-lasting”).

<sup>19</sup> See GAO Report, *supra*, note 17, p. 29.

<sup>20</sup> See S. Rep. No. 105-274, *supra*, note 18, at 7.

<sup>21</sup> See GAO Report, *supra*, note 17, p. 44.

<sup>22</sup> *Id.* P. 28.

<sup>23</sup> In December 2000, the National Fraud Center directed the development of “The Growing Global Threat of Economic and Cyber Crime,” ([www.lexisnexis.com/riskolutions/conference/docs/cyber.pbf](http://www.lexisnexis.com/riskolutions/conference/docs/cyber.pbf)), a report co-authored by Dr. Gary R. Gordon and Dr. George E. Curtis. In the report at page 9, we estimated identity theft losses at \$50 billion per year. We admit that this estimate is a rough approximation but we believe that it is on the conservative side.

<sup>24</sup> “Worker Charged With Stealing Outdated Driver Licenses,” MSNBC.com, December 13, 2001.

<sup>25</sup> *Id.*

<sup>26</sup> Keeshan, Charles, “Carrying a False ID isn’t Just a Kiddie Game,” Daily Herald, November 5, 2001.

<sup>27</sup> *Id.*

<sup>28</sup> Branton, John, “Raid on Identity Theft Ring Also Nets Drugs, Explosives,” pdxguide.com, December 7, 2001.

<sup>29</sup> See GAO Report, *supra*, note 17, p. 29.

<sup>30</sup> *Id.* p. 17.

<sup>31</sup> At the National Fraud Center, our research into the classification of crime enabled us to identify 27 different crimes, listed in Appendix A, that are frequently committed through the use of identity fraud.

<sup>32</sup> Lormel, Dennis M., prepared remarks before the House Committee on Financial Services, hearing on “Dismantling the Financial Infrastructure of Global Terrorism,” October 3, 2001, p. 6.

- 
- <sup>33</sup> Id. p. 6.
- <sup>34</sup> Id. p. 6.
- <sup>35</sup> See GAO Report, *supra*, note 17, p. 34.
- <sup>36</sup> Byers, Stephanie, “Note: The Internet: Privacy Lost, Identities Stolen,” 40 *Brandeis L.J.* 141, 143, Fall 2001. (citing Givens, Beth, “Identity Theft: How it Happens, Its Impact on Victims, and Legislative Solutions (visited Jul. 21, 2000) <http://www.privacyrights.org/AR/idtheft.htm>)).
- <sup>37</sup> Sullivan, Bob, “Russian Linked to Massive ATM Fraud,” *MSNBC.com*, November 29, 2001; “Forensic Detectives; Cybercops. Digital Sleuths,” *Computerworld*, January 14, 2002.
- <sup>38</sup> See, GAO Report, *supra*, note 17, p. 35.
- <sup>39</sup> Kirkpatrick, Michael D., prepared remarks before the United States Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information, hearing on “How New Technologies (Biometrics) Can be Used to Prevent Terrorism,” November 24, 2001, p. 3.
- <sup>40</sup> Lau, Joanna, prepared remarks before the United States Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information, hearing on “Biometric Identifiers and the Modern Fact of Terror: New Technologies in the Global War on Terrorism,” November 24, 2001, p. 2.
- <sup>41</sup> Huddart, Martin, prepared remarks before the United States Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information, hearing on “Biometric Identifiers and the Modern Fact of Terror: New Technologies in the Global War on Terrorism,” November 24, 2001, p. 1.
- <sup>42</sup> Dershowitz, Alan M., “Why Fear National ID Cards?” *New York Times*, October 13, 2001; McCollum, Bill, prepared remarks before the United States House of Representatives Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations Committee on Government Reform, hearing on “Does America Need a National Identifier?” November 16, 2001, p. 4.
- <sup>43</sup> See generally, Corrigan, Katie, prepared remarks before the United States House of Representatives Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations Committee on Government Reform, hearing on “Does America Need a National Identifier?” November 16, 2001.
- <sup>44</sup> Id. p. 3.
- <sup>45</sup> LoPucki, Lynn M., “Article: Human Identification Theory and the Identity Theft Problem,” 80 *Tex. L. Rev.* 89, 95 (Nov. 2001).
- <sup>46</sup> Clarke, Roger, “Human Identification in Information Systems: Management Challenges and Public Policy Issues,” *Info. Tech & People*, Dec. 1994.
- <sup>47</sup> Id. at 6,8.
- <sup>48</sup> See, LoPucki, *supra*, note 46, at 95.
- <sup>49</sup> Id. at 95-96.
- <sup>50</sup> Id. at 96.
- <sup>51</sup> In our previous papers, “Identity Theft: Authentication As A Solution,” and “Identity Theft: Authentication As A Solution – Revisited,” we explained that “authentication,” as we use that term, means the process by which an identity verifier uses information provided by the individual, that pertains to the individual, in order to confirm that the individual is who he or she says they are.

---

<sup>52</sup> O’Harrow, Robert, “Intricate Screening of Fliers in Works,” Washington Post, February 1, 2002; McCartney, Scott, “A ‘Trusted Traveler’ Pass May Be Required In the Cards for Frequent Fliers,” Wall Street Journal, January 30, 2002.

<sup>53</sup> First USA, a subsidiary of Bank One Corp., successfully used such a solution in its credit-card issuing process. Mr. Willox described First USA’s successful application of a knowledge-based authentication solution in his presentation at the Federal Trade Commission’s Identity Theft Victims’ Assistance Workshop, October 24, 2000.

([www.ftc.gov/dcp/workshops/idtheft/transripts/001024-tech.htm](http://www.ftc.gov/dcp/workshops/idtheft/transripts/001024-tech.htm))

<sup>54</sup> Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), Act of October 26, 2001, Public Law 107-45, 115 Stat. 272.

<sup>55</sup> Id. at § 326(a), amending 31 USC § 5318(l)(2)(B).

---

## APPENDIX A

### CRIMES COMMITTED UTILIZING IDENTITY FRAUD

- 1-) APPLICATION FRAUD
- 2-) BANKRUPTCY FRAUD
- 3-) CELLULAR FRAUD
- 4-) CHARITY FRAUD
- 5-) CHECK FRAUD
- 6-) COMMERCIAL LOAN FRAUD
- 7-) COMPUTER FRAUD
- 8-) CONFIDENCE FRAUD/CON GAMES
- 9-) CONSUMER LOAN FRAUD
- 10-) CREDIT CARD FRAUD
- 11-) DRUG TRAFFICKING
- 12-) ELECTION FRAUD
- 13-) FOOD STAMP FRAUD
- 14-) GAMING FRAUD
- 15-) INSURANCE FRAUD/FALSE CLAIMS
- 16-) INVESTORS FRAUD
- 17-) MERCHANTS FRAUD
- 18-) MEDICAL – HEALTH FRAUD
- 19-) MONEY LAUNDERING
- 20-) PYRAMID SCHEMES
- 21-) REAL ESTATE – MORTGAGE FRAUD
- 22-) SECURITIES FRAUD
- 23-) SOCIAL SECURITY BENEFIT FRAUD
- 24-) STUDENT LOAN FRAUD
- 25-) TELEMARKETING
- 26-) TERRORISM
- 27-) WORKERS' COMPENSATION FRAUD