107th Congress
2d Session

SENATE

REPORT
107–133

PHONY IDENTIFICATION AND CREDENTIALS VIA THE INTERNET

REPORT

PREPARED BY THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

FEBRUARY 4, 2002.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
99–010 WASHINGTON : 2002

COMMITTEE ON GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	FRED THOMPSON, Tennessee
DANIEL K. AKAKA, Hawaii	TED STEVENS, Alaska
RICHARD J. DURBIN, Illinois	SUSAN M. COLLINS, Maine
ROBERT G. TORRICELLI, New Jersey	GEORGE V. VOINOVICH, Ohio
MAX CLELAND, Georgia	PETE V. DOMENICI, New Mexico
THOMAS R. CARPER, Delaware	THAD COCHRAN, Mississippi
JEAN CARNAHAN, Missouri	ROBERT F. BENNETT, Utah
MARK DAYTON, Minnesota	JIM BUNNING, Kentucky

JOYCE A. RECHTSCHAFFEN, *Staff Director and Counsel*
HANNAH S. SISTARE, *Minority Staff Director and Counsel*
DARLA D. CASSELL, *Chief Clerk*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

CARL LEVIN, Michigan, *Chairman*	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TED STEVENS, Alaska
RICHARD J. DURBIN, Illinois	GEORGE V. VOINOVICH, Ohio
ROBERT G. TORRICELLI, New Jersey	PETE V. DOMENICI, New Mexico
MAX CLELAND, Georgia	THAD COCHRAN, Mississippi
THOMAS R. CARPER, Delaware	ROBERT F. BENNETT, Utah
JEAN CARNAHAN, Missouri	JIM BUNNING, Kentucky
MARK DAYTON, Minnesota	

LINDA J. GUSTITUS, *Chief Counsel and Staff Director*
KIM CORTHELL, *Minority Staff Director*
EILEEN M. FISHER, *Investigator to the Minority*
MARY D. ROBERTSON, *Chief Clerk*

CONTENTS

PHONY IDENTIFICATION AND CREDENTIALS VIA THE INTERNET

EXECUTIVE SUMMARY

The proliferation of false identification has become a serious public safety issue. False identification documents and credentials can enable criminals to commit a host of crimes ranging from identity theft to bank and credit card fraud and allow them to fund larger and more dangerous criminal activities. Phony identification can also enable criminals to obtain *bona fide,* yet unsupported and unauthorized, identification documents such as driver's licenses. Moreover, criminals may be able to evade law enforcement by hiding behind their false identities. Failing to curb the spread of false identification can have grave consequences, in fact, evidence indicates that some associates of the Al Qaeda terrorist organization may have used false identification and immigration documents.

Also alarming is the ease with which General Accounting Office (GAO) investigators were able to breach security at 21 of the most secure buildings in the United States, including the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and several airports by claiming—falsely, using easily-obtained phony identification—that they were armed law enforcement officers. GAO investigators displayed fake law enforcement badges and phony credentials that they themselves had crafted using graphics software and images culled from Internet websites, and which bore little resemblance to the genuine articles. When the investigators presented themselves at security checkpoints, they were waved around metal detectors and were not screened.

In a similar operation at sensitive Defense Department facilities in May 2001 commissioned by Senator Susan M. Collins, GAO investigators easily penetrated the sites using readily-obtainable false identification—thus demonstrating their vulnerability to unauthorized access by criminals and terrorists. GAO's findings in these multiple penetration tests demonstrate that, in addition to the lax security measures in place at Federal facilities and airports, the Internet and computer technology allow nearly anyone easily to create convincing identification cards and credentials.

In December 1999, under the chairmanship of Senator Susan M. Collins, the Permanent Subcommittee on Investigations began a 5-month investigation into the availability of false identification via the Internet. The Subcommittee's investigation was prompted in part by an e-mail message received by a Subcommittee investigator that solicited her to purchase counterfeit driver's licenses. The Subcommittee began investigating to determine the extent to which false identification could be obtained via the Internet and found

that there are a myriad of websites offering false identification materials.

The Subcommittee examined more than 60 websites offering false identification materials, issued 11 subpoenas for documents and depositions, and interviewed more than 40 witnesses. The Subcommittee also conducted an undercover operation to purchase false identification materials—and received, in turn, several high quality products, including a counterfeit Oklahoma driver's license. Based on the results of this undercover operation, the Subcommittee focused its attention on three website operators each of whom offered high quality products that could be used to produce credible false identification and credentials.

The Subcommittee's investigation found that false identification materials are distributed over the Internet through a number of methods. Some websites offer to make identification documents for customers which are then delivered by mail. Others offer the computer files, known as "templates," necessary to manufacture false identification documents. Customers may purchase access to the templates and download them to their own computers, or purchase a computer disk containing the template files. Still other operators simply offer the templates for free.

Templates are typically graphic files which can be manipulated to hide and/or reveal images and text. Individuals can also add images and text, such as photographs or signatures, to templates in order to customize them. To make a driver's license, for example, an individual would insert a photo and signature, and type in the desired name and address. The individual would then print the document, and laminate it, thereby creating a highly realistic false identification document. A single software template can be used an infinite number of times, by an infinite number of individuals, and can be transmitted via computer disk, or in an instant via the Internet.

As a result of its investigation, the Subcommittee has drawn three general conclusions. First, 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.

Second, the disclaimers that can be found on many websites are at odds with the marketing strategy pursued by the operators of those websites. The Subcommittee found that operators frequently attempted to shield themselves by claiming that their products were "for novelty purposes only." At the same time, however, operators commonly implied that their products were so authentic in appearance as to be illegal—something they clearly considered to be a marketing asset. For example, the Subcommittee found one website that offered a "New Identity Kit" purporting to contain "[e]verything you need to create a new identity for fun!!" yet which encouraged Internet users to order quickly, "before we are shut

down by the authorities." Another website operator informed his customers that his products were for "entertainment and educational purposes only," yet urged them to use the documents on his website to get a job.

Third, 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. For example, one operator, in an attempt to disguise his true location, registered his website in the Philippines and provided an e-mail address that appeared to originate from another small country in the South Pacific. (The Subcommittee determined through his billing records, however, that he was actually located in Kansas.)

The Subcommittee's investigation culminated in a hearing, entitled *Phony IDs and Credentials Via the Internet—An Emerging Problem,* which was held on May 19, 2000. The hearing witnesses were K. Lee Blalack, II, then-Chief Counsel and Staff Director of the Subcommittee; Agent David C. Myers from the Identification Fraud Coordinator for the State of Florida's Division of Alcoholic Beverages and Tobacco (now Lieutenant Myers); Thomas Seitz, a convicted felon; and the Hon. Brian Stafford, Director of the U.S. Secret Service.

In his hearing testimony, Mr. Blalack outlined the scope of the Subcommittee's investigation, and discussed the Subcommittee's case studies of Brett Carreras, Tim Beachum and Tim Catron, who sold false identification materials over the Internet. Lieutenant Myers provided an overview of Internet sales of false identification documents, and detailed several investigations of website operators that he and his team had led, and that the Subcommittee also examined. Thomas Seitz testified about the false identification documents he was able to obtain over the Internet, and the crimes he was able to commit using these phony documents. (These actions resulted in his conviction on four felony counts, a 3-year State sentence and a 7-month Federal sentence.) Finally, Director Stafford testified about the proliferation of Internet crime and how the Internet facilitates identity theft and other serious crimes through the use of false identification documents. He also outlined the role of the U.S. Secret Service in trying to curb such activity.

The Subcommittee's hearing made clear that technological developments during the past few years have significantly increased the dangers associated with the production and marketing of phony identification documents. Today, both the necessary skills and materials are well within the reach of a growing number of people. As then-Chairman Collins noted in her opening statement:

> "These counterfeit documents are relatively easy to manufacture. With only a modest understanding of the Internet and $50 worth of supplies purchased from an arts and crafts store, one can design authentic-looking identification documents within a few hours or even minutes." [1]

[1] *Phony IDs and Credentials Via the Internet: An Emerging Problem:* Hearings before the Permanent Subcommittee on Investigations, Senate Committee on Governmental Affairs, 106th

Continued

Moreover, it is becoming even easier to obtain and create false identification documents, which can then be used for a wide variety of improper and illegal purposes. Senator Carl Levin noted in his opening statement, for example, that false identification documents are

> "often now being used to carry out improper or criminal activities—to obtain fraudulent loans, to evade taxes, to establish a new identity, to steal another individual's identity, to defraud Federal and State Governments, to misrepresent one's residence or place of birth or age for any variety of purposes." [2]

Indeed, a criminal can use phony identification documents and credentials as so-called "breeder" documents, as a means of gaining access to *bona fide* identification materials. Seitz obtained a phony birth certificate, for instance, to obtain a State identification card, which while itself authentic (insofar as it was properly issued by the relevant authorities), was based on false supporting documents and contained false information. Through these means, Seitz obtained unauthorized yet "authentic" documents, which are particularly difficult to detect. These "authentic" documents can then be used to commit a host of crimes, including bank fraud, as Seitz unfortunately demonstrated. Although at the time of this report investigations into the terrorist atrocities of September 11, 2001, are still in the early stages, it appears that some individuals associated with these acts may also have used false supporting documents to obtain "authentic" false identification.

The Internet has visibly changed the false identification industry. In his testimony before the Subcommittee, Lieutenant Myers estimated that 30 percent of the false identification documents his office seized during the year 2000 had been obtained via the Internet—up from only about 1 percent just 2 years previously. Moreover, Lieutenant Myers expected this figure to rise to between 60 and 70 percent for 2001.[3] Indeed, Trent Sands, the author of a recent book on false identification, claims that the Internet should be credited with reviving the false identification business:

> "The Internet has breathed new life into the world of false identification. Many new companies are springing up to meet the needs of those who want documentation saying they are someone else. * * * The robust health of the mail-order and Internet identification business is in stark contrast to the situation of just a few years ago."

Since the Subcommittee began its investigation and began contacting website operators, most of the individuals examined, including Tim Catron and Tim Beachum, have removed their websites from the Internet. Others, such as Brett Carreras, have curtailed their activities. The Subcommittee has also made referrals of potential violations of Federal and State law to the appropriate members of the law enforcement community, urging authorities to in-

---

Congress, 2nd Session (May 19, 2000) [hereinafter "Hearing record"], at 2 (remarks of Senator Collins).

[2] *Id.* at 4 (remarks of Senator Carl Levin).

[3] *Id.* at 20 (testimony of Lieutenant David C. Myers).

vestigate further the activities of several individuals involved with manufacturing and distributing false identification documents. Nevertheless, operators continue to spring up to take the places of those who have closed their websites and offer false identification and credentials over the Internet, although most of these new operators are located abroad.

Accordingly, the Subcommittee considered means of curbing this emerging problem, and in July 2000, then-Chairman Collins introduced legislation designed to address the problem of counterfeit identification documents. This legislation, the Internet False Identification Prevention Act of 2000 passed the Senate and the House of Representatives and was signed into law on December 28, 2000. This statute, Public Law 106–578, effected a number of changes in current law, including: (1) establishing a multi-agency coordinating committee charged with encouraging more enforcement of existing criminal laws by dedicating investigative and prosecutorial resources exclusively to this emerging problem; (2) modernizing several portions of existing Federal law to ensure that it is suited to the Internet age and the technology that is associated with it; and (3) making it easier to prosecute those criminals who manufacture, distribute, or sell counterfeit identification documents by closing the legal loophole that had allowed them to use easily-removable disclaimers in an attempt to shield their illegal conduct from prosecution through a claim of "novelty." Through aggressive law enforcement activity, and continued Congressional attention and oversight, the Subcommittee hopes and anticipates that it will be possible dramatically to decrease the number of crimes committed using false documents.

I. *Introduction*

A. *Summary of Investigation*

The Subcommittee's investigation was prompted in part by an e-mail message received by a Subcommittee investigator that solicited her to purchase counterfeit driver's licenses.[4] The Subcommittee began investigating to determine the extent to which false identification could be obtained via the Internet. Unfortunately, it quickly became apparent that there are a myriad of websites offering false identification materials.

From mid-December 1999 to mid-May 2000, the Subcommittee discovered approximately 60 websites offering to manufacture and sell false identification documents or to provide the means to manufacture false identification documents. These sites were not hard to find: the Subcommittee located them by using major search en-

[4] This issue first came to the Subcommittee's attention when Subcommittee Investigator Eileen Fisher received an unsolicited e-mail message entitled, "Authentic Confidential ID's!!" The e-mail message stated as follows:

> "Ever wanted a driver's license that pases [sic] all the "tests"? Now you can have a Driver's License from any State no questions asked! Former employees of the Department of Motor Vehicles are now making Driver's licenses exactly 100% like the ones the DMV makes, complete with Holgrams [sic] and Magnetic Strips."

The message asked Investigator Fisher to send $15 in payment for the fake driver's license. *See* Hearing record, *supra,* at Exhibit 22. The individual responsible for this e-mail, Greg Dodson, agreed to a consent judgment on May 19, 2000, in a lawsuit brought by ASD.com in the U.S. District Court for the Middle District of Tennessee. The terms of the consent judgment require Dodson to pay statutory damages under the Tennessee anti-spamming statute of $10,000 plus attorney's fees.

gines, examining the links on websites, and reviewing messages posted on several discussion boards. The websites primarily offered to manufacture or provide information about State driver's licenses, with some operations offering to manufacture or provide information about birth certificates, government identification cards, Social Security cards, college transcripts, and other identification documents.

The Subcommittee then reviewed in great detail approximately 15 websites that offered false identification information. These websites were selected based on the type and quality of documents offered, the methods used to sell such documents, and the physical location of website operations. As part of the Subcommittee's review, the Subcommittee placed orders under an assumed name to seven websites for the false identification products that they offered. The Subcommittee received materials from three of the websites. A summary of these orders and results is provided in Table 1:

Table 1—Orders of False Identification Materials

Company/Individual	Product Ordered	Cost	Result
American Photo Company[a]	Georgia driver's license with hologram.	$225	No product received.
NoveltyID4U[a]	Social Security card	$58	No product received.
Mike Burton	Maine driver's license	$75	No product received.[b]
The ID Shop/Robert Sek	Oklahoma driver's license.	$100	Received false identification card closely resembling an Oklahoma driver's license.
J&J Enterprises/Josh Dansereau	Connecticut driver's license.	$58	No product received.[c]
Bestfakeids/Tim Beachum	Novelty ID Kit	$30	Downloaded files containing identification documents.
Fakeid.net/Brett Carreras	Monthly access to premium files.	$12.95/month	The Subcommittee had access for several months to these materials, which included templates for 13 State driver's licenses, the seal of the Department of Health and Human Services (which is used on a Social Security card), and a template for a Canadian driver's license.

[a] It appears that the same individual, John Carroll, operates both companies, and possibly several others including phonyid.com.

[b] When Subcommittee investigators contacted Burton, he admitted that he did not send the requested fake driver's license because he was attempting to defraud customers by taking their money without shipping the goods promised. Following the Subcommittee's referral of this case to the appropriate law enforcement authorities in Fond du Lac, Wisconsin, Burton was charged with petty theft by fraud and fined approximately $200. He also disestablished a website he had operated offering instructions on how to alter a driver's license, shredded his own altered Wisconsin driver's license at the direction of authorities, and returned $75 to the Subcommittee.

[c] Dansereau was arrested by Florida agents in November 1999. Nevertheless, the Subcommittee's money order was deposited into his account in February 2000. In June 2000, Dansereau signed a notarized affidavit confirming his statement to the Subcommittee that since his arrest he has returned all orders for false identification documents.

The identification materials the Subcommittee received took different forms. After the Subcommittee mailed to the operator of one website a photograph representing a fictitious person with an address in Oklahoma, asking that the false identification document be delivered to an address in Maryland, the Subcommittee received a high quality identification card[5] that closely resembled a driver's license of the State of Oklahoma. (This false identification document is further described in Section III.A.(1).) The Subcommittee used a credit card to purchase access to templates[6] and informa-

[5] *See* Hearing record, *supra*, at Exhibit 9 (false Oklahoma driver's license).

[6] Templates are computer files that are frequently used to manufacture false identification documents. See Section II.B.(1).

tion from two other websites that can be used to manufacture false identification documents. These websites are described in Sections III.A. (2) and (3) of this report. The Subcommittee also obtained templates and other information on false identification from websites that did not charge for their products.

The Subcommittee experienced difficulty in locating and obtaining the cooperation of the operators of several of the websites under review. As detailed in Section III.E.(2) of this report, many of those responsible for these websites hid their associations with the website or, when identified, were unwilling to provide verifiable information to the Subcommittee. Some websites appear to be operated by individuals or companies located outside the United States, making it difficult for the Subcommittee to compel the production of information.

In the cases of several websites, the Subcommittee found the sales of false identification materials to be significant, as illustrated in Table 2:

Table 2—Revenues/Orders of Websites Offering False Identification Materials

Company/Individual	Est. Dates of Operation	Dates of Revenue/ Order Information	Revenues	Orders
The ID Shop/Robert Sek	11/30/99–2/00	11/30/99–2/00	$1,000,000 [a]	21,000 [a]
fakeid.net/Brett Carreras	7/28/98–present	10/18/98–12/22/98	$8,239 [b]	621 [b]
Bestfakeids/Tim Beachum	3/17/99–5/00 [c]	3/17/99–3/24/00	$31,305 [d]	1,294 [d]
Infoworld/Jeremy Martinez	10/99–5/00 [c]	1/1/99–3/30/00	$23,728 [d]	1,177 [d]
fakeidzone/Tim Catron	10/98–2/00	11/99–1/00	$12,250 [b]	652 [b]
J&J Enterprises/Josh Dansereau	6/99–9/99	6/99–9/99	$3,000 [d] – $250,000 [a]	100 [e]

[a] Estimates from law enforcement reports.
[b] Information provided by Verotel, the company recording billing information.
[c] Website was operational as of May 19, 2000. However, it appears to have been taken down at some point between the Subcommittee's hearing and the release of this report.
[d] Company-supplied information.
[e] Dansereau claimed that he manufactured about 100 false identification documents. Law enforcement officials believe Dansereau failed to provide products to many customers.

B. *Methods of Using the Internet to Find False Identification Materials*

The Internet offers users an ever expanding multitude of information.[7] With over 35 million domain names registered as of June 4, 2001,[8] the Internet provides users with an opportunity to find information on virtually any subject. Individuals across the world are using the Internet in ever increasing numbers, with one source estimating the number of Internet users worldwide as 414 million in 2000 and predicting an increase to 1.17 billion by the year 2005.[9]

The vast array of information sources on the Internet means that most Internet users do not know the location of websites that may contain information on a topic of interest to them.[10] Internet users

[7] The Internet is also called the World Wide Web, a term which is often shortened to simply "the Web." It is a linked collection of electronic documents stored on computers called servers.
[8] Netnames Int'l Ltd., *Netnames* (visited June 4, 2001) **http://www.netnames.com.**
[9] Computer Industry Almanac, *Internet Users/Wireless Users* (visited June 4, 2001) **http://cyberatlas.internet.com.**
[10] Websites, or pages, are located by an "address" known as a domain name, an Internet Protocol (IP) address, or a Universal Resource Locator (URL). This address is sometimes called the

Continued

thus routinely search for information using "search engines," [11] programs which automatically search large sections of the Internet in order to provide the user with a list of websites likely to contain information relevant to the user's request. After the user has entered one or more words describing the subject matter of interest, these search engines use different techniques to identify websites with a high probability of containing the requested information. Search engines may identify relevant websites through comparison of the user's word description with terms on a website or with descriptive terms, frequently called "keywords," provided by the creator of the website in order to guide or attract users to the website. Based on this comparison, search engines provide an Internet user with a list of websites. This list is often arranged in order of likelihood of containing relevant information, and may provide a short description of the information included on each site. The search engine results page displays the address of each page found as a result of the search, and allows the user to move directly to each site with a simple click of the mouse.[12] As the Subcommittee demonstrated, these user-friendly and often very powerful search techniques make it easy for Internet users to discover and access websites offering a variety of false identification documents.

C. *Earliest Websites Offering False Identification Information*

The ever-changing nature of the Internet, and the fact that web pages are often not preserved for later retrieval, prevent documentation by the Subcommittee of the earliest websites created containing information about false identification materials. Website "domain names" are often sold or transferred to different individuals or companies, and may be used for an entirely different purpose at different times. The Subcommittee's investigation was thus unable to determine with great certainty which operators first used the Internet to offer false identification information.

The earliest information about manufacturing false identification appears to originate from three websites. A site named "Blur of Insanity," which currently describes itself as "The #1 College Entertainment Website," [13] is mentioned on an Internet discussion board [14] as having been one of the first sites to display identification templates.[15] According to other messages on a discussion board,[16] an individual using the name "Cycore" provided information about false identification materials on a site offered on a web page provided through America OnLine (AOL)—at least until that company allegedly dismantled the site. A third site, "fake-id.com," operated by John DeMayo, was registered with Network Solutions

---

name of the site, its address, or its location. Entering the URL of a web page through a web browser or clicking on a link allows the user to access that page through its server.

[11] A "search engine" is a web page that uses computer technology to find and display other web pages relating to the information requested.

[12] *See e.g.*, Hearing record, *supra,* at Exhibit 28 (search results for term "fake ID" when using Excite.com search engine, **http://www.Excite.com).**

[13] *See* "Blur of Insanity," (last visited Dec. 15, 2000), at **http://www.blurofinsanity.com.**

[14] *See* "Fake ID Conversation," **http://www.carreras.net/discus** (post by "Allfree" on Oct. 15, 1999).

[15] A "template" is the term given to a document, often in the form of a computer file that is able to be manipulated, and may contain both graphic images and text, and that closely resembles the common features of an official identification document.

[16] *See* "Fake ID Conversation," **http://www.carreras.net/discus** (post by "Webhost" on Oct. 16, 1999).

on October 2, 1997. This site reportedly contained a variety of templates and information about the driver's licenses of many different States. Individuals obtaining these templates and information about the formats of State driver's licenses would then have the ingredients needed to manufacture false identification. Although the Subcommittee was unable to obtain specific information about the false identification information presented on these early websites, it does appear that the use of the Internet to manufacture and market counterfeit identification documents dates at least to the mid-1990s.

D. *Legal Framework*

(1) *Federal Legislative History*

Almost 20 years ago, in the fall of 1982, the Subcommittee held 3 days of public hearings examining the use of counterfeit identity documents to defraud Federal benefit programs.[17] These hearings came on the heels of a series of reports demonstrating the growing problems caused by false identification. Following the hearings, Congress enacted 18 U.S.C. §§ 1028 and 1738. These two laws are the primary Federal statutes that relate to the availability of false identification on the Internet. Section 1028 imposes penalties for the production or use of false identification documents, as well as for the possession of document making implements with the intent to use them for an illegal purpose. Section 1738, which was repealed in 2000, imposed a misdemeanor penalty for possessing certain identification documents that do not bear a specified disclaimer.

Section 1028 imposes felony sanctions of between 3 to 25 years in jail, depending how the false identification document is used, for:

- the knowing, unauthorized production of an identification document, or false identification document;
- the transfer of an identification document or false identification document, knowing that it was stolen or produced without lawful authority;
- the possession with intent to use unlawfully or to transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor) or false identification documents;
- the possession of an identification document (other than one issued lawfully for the use of the possessor) or a false identification document with the intent that such document be used to defraud the United States;
- the possession, production, or transfer of a document-making implement with the intent that the implement be used in the production of a false identification document or another document-making implement;
- the possession of an identification document that is or appears to be an identification document of the United

[17] *See generally, Federal Identification Fraud:* Hearings before the Permanent Subcommittee on Investigations, Senate Committee on Governmental Affairs, 97th Congress, 2nd Session (June 15–16, Sept. 23, 1982).

States, which is stolen or produced without lawful authority, knowing that the document was stolen or that its production was unauthorized; and

- the unauthorized transfer of a means of identification of another person with the intent to commit, aid, or abet any unlawful activity that violates Federal law or is a felony under State law.

Section 1028 applies only where (1) the identification document or false identification document is or appears to be issued by or under the authority of the United States, or the document-making implement is designed or suited to making such an identification document; (2) the offense involves the knowing possession of an identification document (other than one lawfully issued for the use of the possessor) or a false identification document intended to be used to defraud the United States; (3) the prohibited production, transfer, possession or use is in or affects interstate or foreign commerce; or (4) the means of identification, identification document, false identification document, or document-making implement is transported in the mail.[18]

Section 1738 made it a misdemeanor punishable by up to 1 year in jail for anyone in the business of furnishing identification documents, acting in furtherance of that business, to use the mails for the

> "mailing, carriage in the mails, or delivery of, or [transportation] in interstate or foreign commerce, any identification document * * * (1) which bears a birth date or age purported to be that of the person named in such identification document; * * * (2) knowing that such document fails to carry diagonally printed clearly and indelibly on both the front and back "NOT A GOVERNMENT DOCUMENT" in capital letters in not less than 12-point type."[19]

An "identification document" is defined as "a document which is of a type intended or commonly accepted for the purpose of identification of individuals and which is not issued by or under the authority of a government."[20]

(2) *Loopholes Caused by Advances in Technology*

The Subcommittee found that the substantial majority of false identification prosecutions have been brought under § 1028, while no prosecutions have been brought specifically under § 1738, perhaps because § 1738 provided only for misdemeanor penalties. Moreover, the Subcommittee's review of the case law under § 1028 did not find any prosecutions involving the sale of false identification documents over the Internet. Witness testimony at the Subcommittee's hearing indicated, however, that the number of crimes committed involving false identification is growing, and that the number of prosecutions has not kept pace. Not only did the statute need updating, the Subcommittee concluded, but law enforcement's attention also needed to be refocused on this crime.

---

[18] 18 U.S.C. § 1028.
[19] 18 U.S.C. § 1738(a).
[20] *Id.* at § 1738(b).

Under § 1028, the courts have looked to statutory language, past decisions, and legislative history to determine the appropriate scope of the terms "identification document" and "document-making implement." The cases indicate that the term "identification document" applied to completed and blank birth certificates, driver's licenses, and Federal and State identification cards.[21] The statutory definition of a "document-making implement" included

> "any implement, impression, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement."[22]

The case law suggests that this language has been applied to a wide range of materials outside the Internet context, but it is unclear whether the existing statutes would cover computer files or false-identification software template files. Specifically, it was unclear whether templates, which are used in a large number of those false identification documents transmitted over the Internet, constitute a document or a document-making implement—or whether they were covered at all under the original statutory definitions. The Subcommittee concluded that new legislation was needed to ensure that such computer technology is within the ambit of the statute, particularly because it is the method of choice of today's false identification manufacturers.

The Subcommittee found that people producing false identification cited the disclaimer language in § 1738 in claiming to be operating in compliance with the law. For example, Robert Sek of "theidshop" required that his customers sign an agreement not to tamper with the product he sent them. He then mailed his customers an identification card sealed in an easily-removable plastic pouch that bore the requisite disclaimers. The identification card inside the pouch bore merely a disclaimer in tiny print.[23] Through these means, Sek sought to insulate himself from liability by creating a product that appeared to comply with § 1738, but in fact was easily alterable to circumvent the statute.

For these reasons, it was apparent following the Subcommittee hearing that the statutory definitions of prohibited items needed to be updated to cover today's technology, and that law enforcement's attention need to be refocused on false identification crimes. Speaking from his position as one on the front lines of the effort to curb phony identification documents, for example, Lieutenant David C. Myers, the Identification Fraud Coordinator for the State of Florida's Division of Alcoholic Beverages and Tobacco, testified to the difficulties he encountered, noting that false identification website operators keep reappearing on the Internet, a problem he suspected rises from loopholes in the current legal code.[24] After hearing this, Senator Collins noted:

---

[21] *See generally United States v. Alejandro,* 118 F.3d 1518 (11th Cir. 1997); *United States v. Rohn,* 964 F.2d 310 (4th Cir. 1992).

[22] 18 U.S.C. § 1028(d)(1).

[23] *See* Hearing record, *supra,* at Exhibit 10 (*Fake ID Man Message Board* **http://pages.eidosnet.co.uk/fakeidman/** (post by "Mexican311" on Mar. 17, 2000)). This post details the ease with which the disclaimer on the identification card may be removed.

[24] *Id.* at 22 (testimony of Lieutenant Myers).

> "I am more convinced than ever that we need a crackdown by all levels of law enforcement on this area and that we need to evaluate very closely whether Federal law and penalties are sufficient to deter the proliferation of these websites." [25]

(3) *Internet False Identification Prevention Act of 2000*

On July 26, 2000, Senator Collins introduced S. 2924, the Internet False Identification Prevention Act of 2000, in an effort to curb the proliferation of websites that distribute counterfeit identification documents and credentials over the Internet. The bill was intended to accomplish this by promoting a coordinated effort to improve the Federal Government's ability to stem the use of false identification documents, creating a law enforcement coordinating committee to focus on false identification, updating existing law to reflect technological advances, and encouraging law enforcement to prosecute this serious and growing problem. On December 15, 2000, after incorporating several minor modifications to the version that had previously passed the Senate, the U.S. House of Representatives passed the Internet False Identification Prevention Act of 2000. Thereafter signed by the President, this bill became Public Law 106–578 on December 28, 2000. It entered into effect on March 28, 2001.

Among its provisions, the new law authorizes a multi-agency coordinating committee to investigate and prosecute the manufacture and distribution of false identification documents. The coordinating committee includes representatives from the Treasury Department, the Justice Department, the U.S. Secret Service, the FBI, the Social Security Administration, and the Immigration and Naturalization Service (INS). This coordinating committee is expected to operate like the Office of Internet Enforcement at the Securities and Exchange Commission (SEC), except that it would file criminal rather than civil actions and would be a multi-agency organization. This coordinating committee shall exist for at least 2 years, with the President having the authority to continue it for such additional time as may be deemed necessary. At the end of each year of the coordinating committee's existence, the Attorney General and Secretary of the Treasury shall report to the House and Senate Judiciary Committees on the investigation and prosecution of crimes involving false identification, and make recommendations for more effective investigation and prosecution.

Second, the new law was designed to amend § 1028 in order to bring this primary law on false identification in line with current technology in several ways. The legislation modifies the existing definition of "document-making implement," for example, to include computer templates and files that are now frequently used to create counterfeit identification documents from the Internet.

Third, the new law aims to close a loophole which allowed a person to transfer (e.g., through a website or e-mail), either false identification software templates or actual finished documents. The law's new provision thus expands the definition of "transfer" to include selecting, placing, or directing the placement of an identifica-

[25] *Id.* at 30 (remarks of Senator Collins).

tion document, false identification document, or document-making implement in an online location where it is available to others. This should ensure that offering a false identification document or template for download on a website is considered an illegal act.

Fourth, the new law repeals § 1738, thus ending individuals' ability to use alterable disclaimers in legally producing identification documents that include the age or birth date of an individual. The effect of repeal of § 1738 is that it will no longer be legal to manufacture and sell false identification products even if they display the previously-required "NOT A GOVERNMENT DOCUMENT" disclaimer. As the Subcommittee's hearing revealed, this type of disclaimer can be fashioned so as to be easily removable on both computer templates and counterfeit identification documents. It is now illegal to produce, possess, or sell any identification document that resembles an identification document issued by any government entity; any such activity will be a felony.

It is the Subcommittee's hope that this new law will also focus attention on the growing problem of Internet-facilitated false identification. This alone may help rein in the more visible operators, for shedding light on this industry does appear to be at least a temporary deterrent. Lieutenant Myers testified at the hearing, for example, that:

> "Probably the biggest impact that we have had on the Internet as I monitor it and have for many years is the work done by your own Subcommittee's investigators. They had a dramatic impact on those on the Internet. Not even knowing their investigation was going on, I could see that the activity on the Internet as it related to false ID was going through some changes." [26]

The Subcommittee hopes that the combination of its work on the subject and the legislation to curb the manufacture and distribution of false identification documents over the Internet, along with renewed attention from law enforcement will decrease the number of crimes committed using the false documents.

II. *The Subcommittee Investigation*

A. *Methods Of Providing False Identification Materials By Internet Sites*

The Subcommittee's investigation found two primary methods by which the operators of websites provide false identification materials: some simply provide their customers with the tools they need to produce their own false identification. These products are generally mailed in disk form to the customer, or more frequently, transmitted via the Internet, or available for downloading. Other website operators produce a completed false identification document for their customers themselves, which they deliver to the customer through the mail.

---

[26] *Id.* at 21–22 (testimony of Lieutenant Myers).

(1) *Some Websites Offer False Identification Information and Tools*

Some website operators offer to mail customers a disk containing computer files. The operator of *fakeidzone.com,* Tim Catron, used the following language to promote his products:

> "Our novelty id kit's allows anyone to make a new identity. Maybe you would like to be able to spot fake id's [sic] for your job, or you need a new novelty birth certificate, or maybe you want to make some money selling novelty id's. Everything you need is right here! You will get full instructions with details on how to use your kit—as well as hundreds of templates, and tech support if needed." [27]

These website operators usually require payment by mail and provide the disk via return mail. Such sites are frequently unable or unwilling to use a third party for billing, and customers using such sites may not have credit cards or prefer to send their payment using untraceable methods such as cash or money order.

The operator of the website *fakeid.net,* Brett Carreras, promoted his site as "[t]he world's first and finest site devoted solely to fake ID information." This website contained free information such as State seals, coded numeric information on State issued identification, and templates that would assist an individual to create false identification. *Fakeid.net* also sold membership access to "premium" files containing high quality templates of State driver's licenses. Website operators offer files for the customer to download, maintain accounts with credit card or billing companies, and customers charge their purchase to a credit card, pay by telecheck, or pay through their telephone bill. Once the billing company has confirmed the purchase, an authorization code is provided to the customer for access to the files containing the information about false identification documents.

Other websites offer, without charge, files available for downloading that contain false identification materials. For example, one website operator promoted the products offered with the following statement: "Welcome to the Fake ID Archive! Here you will find everything you will need to make your own Fake ID." [28] The Fake ID archive's product list included high quality, layered templates that customers could use to manufacture false identification. While the operators of these websites appear to be offering their products for free, their sites may generate income by linking to other web pages whose owners pay a fee for directing potential customers to them.

(2) *Some Websites Offer to Manufacture False Identification*

Some websites offer to make identification documents for customers. The operator of *theidshop.com,* Robert Sek, offered to provide customers with PVC plastic identification cards [29] that closely resembled State driver's licenses. The Subcommittee purchased a

---

[27] *See* Hearing record, *supra,* at Exhibit 32b (Tim Catron, *Fake ID Zone* (visited Jan. 3, 2000) **http://www.digitalhideout.com/idkit.html**) (original punctuation and spelling preserved).

[28] *Fake ID Archive* (visited Apr. 21, 2000) **http://www.fakeids.cjb.net.**

[29] Polyvinylchloride, commonly known as PVC, is a widely used type of plastic. PVC is frequently used to make cards such as identification badges and credit cards.

phony Oklahoma driver's license from Sek, and found that the identification was high quality, and closely replicated a *bona fide* Oklahoma driver's license. The Subcommittee's purchase is detailed in Section III.A.(1). Sek's web page described his products as follows:

> "The ID Shop is proud to be the first Id website to ever offer PVC plastic holographic ID's. These are the highest quality novelty ID's money can buy. They also come with many added security options such as holograms." [30]

The operator of *fakeids.org,* Josh Dansereau, similarly promoted his products as follows:

> All of are ID's are the new plastic credit card style, they come with a working magnetic strip at no extra charge. No one will question these Ids, even put to the book test * * * they pass. We get e-mails everyday about how great they work. Our Ids are made to very strict standards, you will be completely satisfied.[31]

These websites ask the customer to send the information that he or she wants on the identification document along with a picture, signature, and payment. The operator of the website manufactures the new identification, makes no attempt to verify that the information is true, and sends the customer the false identification document via return mail.[32]

B. *Types of False Identification Materials Available on the Internet*

(1) *Templates and Other Tools*

Some websites offer template and other tools that aid individuals in the manufacture of false identification documents. Templates are computer files that are frequently used to manufacture false identification documents. Templates are typically layered graphic files that can be manipulated to hide and reveal images and text. Layering a template enables the customer to replicate closely a feature on a State driver's license, such as a signature or seal, that appears to cover a portion of a picture, as each layer contains a portion of the entire image, such as the seal or signature. Individuals can also add images and text such as photographs or signatures to templates in order to customize them. To make a driver's license, for example, an individual would insert a scanned photograph and signature, and type in the correct name and address. Then the individual would print the document and laminate it. Because templates are merely electronic code indicating the graphic patterns of the desired document, one template can effectively be used an infinite number of times, by an infinite number of individ-

---

[30] *See* Hearing record, *supra,* at Exhibit 31 (Robert Sek, *PVC Plastic Id's* (visited Jan. 27, 2000) **http://www.theidshop.com**).

[31] Josh Dansereau, *Gallery* (visited Nov. 9, 1999) **http://www.fakeid1.com/gallery.htm** (original punctuation and spelling preserved).

[32] Identification documents are sent by return mail, at least, when the operator of the website is not simply defrauding customers of their money by providing no product whatsoever. As noted in Table 1, for example, the website operated by Mike Burton was designed to elicit orders for false identification products that Burton never intended to provide. Such activity is not a false identification crime, but instead constitutes simple fraud.

uals, and can be transmitted easily via computer disk, or virtually instantaneously over telephone lines via the Internet.

In the case of the older versions of the Maine driver's license, for example, both the State seal and the signature of the Secretary of State overlap the picture of the license holder. This is a security feature that helps prevent the physical alteration of an actual license by the simple expedient of replacing the original picture, since such tampering would cover a portion of the seal and signature. A layered computer template allows a new picture to be inserted "under" the seal and signature so that it duplicates an official license. A simple "mouse click" in the program deletes the seal and signature block. After the user inserts the desired picture, the seal and signature block are simply reapplied as a layer above the picture.[33] In this manner, users are able to defeat many of the security features that authorities have put in place.

With sophisticated templates and printers available, it is within the reach of a growing number of people to produce false identification and credentials. As Senator Collins noted in her opening statement at the Subcommittee hearing:

> "These counterfeit documents are relatively easy to manufacture. With only a modest understanding of the Internet and $50 worth of supplies purchased from an arts and crafts store, one can design authentic-looking identification documents within a few hours or even minutes." [34]

Some websites offer other security features or devices that, when added to a template, result in a more realistic identification document. Websites provide bar codes, or computer programs that generate a bar code, which may then be used as part of a counterfeit driver's license. Lieutenant Myers noted in his testimony at the hearing that website operators are keeping pace with the security features that States have been adding to their identification documents. "Things like bar codes and even two-dimensional bar codes that some States are going to," he noted, "are easily generated off the Internet. There are several sites that assist you in generating these security features." [35] Other websites reproduce the seal or flag used by States on their driver's licenses.[36]

Other websites provide a computer program that enables the user to generate a realistic driver's license number. Many States use special coding in their driver's license numbers, allowing verification of the license by matching the driver's license number with certain characteristics of the owner. For example, the first letter of the driver's license number may correspond to the first letter of the owner's last name. Other digits may correspond to the month and year of birth, sex, or eye color. These websites offer a program

---

[33] *See* Hearing record, *supra,* at Exhibits 4 and 5. Exhibits 4 and 5 show, respectively, a template for a Maine driver's license without a photo in the photo layer, and a template for a Maine driver's license with a photo in the photo layer.

[34] Hearing record at 2 (remarks of Senator Collins).

[35] *Id.* at 20–21 (testimony of Lieutenant Myers); *see also, e.g.,* Jeremy Martinez, *New Identity Kit* (visited Dec. 10, 1999) **http://www.newid.ultramailweb.com.**

[36] *See e.g.*, Brett Carreras, *Fake ID.Net* (visited May 12, 2000) **http://www.fakeid.net.**

that replicates a driver's license number that corresponds to the code of the State selected for a phony driver's license.[37]

Other websites offer Social Security number generators or explain the method used by the Social Security Administration in issuing actual Social Security numbers. This numerical coding, corresponding to the State and year of birth, provides another method to verify the apparent identity of an individual. Such information, when available and used by those manufacturing false identification documents, can be used to create a Social Security number that appears to match a counterfeit identity.[38]

(2) *False Identification Documents*

(a) *State Driver's Licenses and Identification Cards*

The Subcommittee found that many websites offer to manufacture, or provide information that would allow the customer to manufacture, a document that would closely replicate the driver's licenses of various States. Most such websites are illustrated by pictures of the products that they offer,[39] usually images of State driver's licenses. These images often include the picture of an individual or appear to be actual licenses, with either the picture or name of the individual removed. In other instances, the images shown are copied from samples appearing in a book published for law enforcement and private sector businesses that describes the features of State driver's licenses and identification cards.

The Subcommittee's investigation found that the quality of the materials manufactured or offered by each website varied considerably. Some websites produced documents that closely replicated the driver's license of a State in graphic images, size, shape, format, color, typeface, and placement of features such as State seals and signatures, while others clearly bore little resemblance to the genuine article. Lieutenant Myers noted in his testimony that phony identification documents are available via the Internet for all 50 U.S. States and many government agencies.[40] Websites manufacturing high quality identification documents frequently attempt to duplicate security features such as "ghost" pictures, holograms, and bar codes or magnetic stripes. These security features are very valuable to manufacturers, as they contribute to the realistic look of the counterfeit document.

As Lieutenant Myers testified at the hearing, these security features now pose little difficulty to counterfeiters:

> "Some of the features on the license * * * such as the what we call a ghost image picture, those were very, very difficult to reproduce in years past due to the technology that we had at that time. Now it is very simple."[41]

In fact, Lieutenant Myers added, "our [law enforcement] training programs have to be updated virtually every month to come up

---

[37] *See e.g.,* Tim Catron, *Fake ID Zone* **http:www.digitalhideout.com/idkit.html**; Jeremy Martinez, *New Identity Kit* **http://internetwebhosting.com/newid/iddownload**; *Novelty Fake ID Info CD* (item 286156827) **http://www.ebay.com.**

[38] *See e.g.*, Jeremy Martinez, *New Identity Kit* (visited Dec. 10, 1999) **http://www.newid.ultramailweb.com.**

[39] *See, e.g.,* Hearing record at Exhibit 31.

[40] Hearing record, *supra,* at 13 (testimony of Lieutenant Myers).

[41] *Id.* at 20 (testimony of Lieutenant Myers).

with new technologies that are being used."[42] No longer are individuals who devote many hours of study and practice the only ones able to reproduce these once effective security features. Senator Collins observed during the hearing that

> "Many States, such as Connecticut, have added * * * security features * * * for example, one of the security features is the shadow picture and the bar code. But my staff was able to replicate that in a way that makes it virtually indistinguishable from a real Connecticut license."[43]

Some websites also offer documents that closely resemble a State driver's license, but are missing one or more security features. Such documents are still quite effective for commercial activities and also might be used to obtain other authentic documents, because only trained personnel are likely to notice the subtle differences. Trent Sands, author of the book, *Fake ID by Mail and Modem,* advises his readers to capitalize on this lack of training:

> "Mail order documents can be used effectively in situations where the ID cannot be verified by the person you are presenting it to. Consider the case of where an individual wants to open a bank account * * *. The bank clerk will accept the document without any problem if it looks real."[44]

Moreover, there are a multitude of State identification cards in circulation, employing a wide variety of security features. This is a serious problem about which Lieutenant Myers testified at the hearing, noting that

> "there are over 200 active State identification cards and driver's licenses due to the fact that most States have an ID card and driver's license and have valid older formats also. So in order for a law enforcement person to be able to recognize all these features in areas like Florida, where we have a lot of out-of-State people, it is almost impossible to have everyone at the expert status in order to identify all these types of legal identification."[45]

(b) *Other Identity Documents*

Some websites actually offer to manufacture a counterfeit Social Security card. The card issued by the Social Security Administration is not intended to be an identification document, and thus contains only an individual's name and Social Security number. Older Social Security cards feature no real security features, although recently issued cards are more resistant to forgery.[46] The Subcommittee also found a wide range of other identity documents available from websites, such as press credentials, a travel agent

---

[42] *Id.* at 21 (testimony of Lieutenant Myers).
[43] *Id.* at 20 (remarks of Senator Collins).
[44] Trent Sands, *Fake ID by Mail and Modem,* at 23 (2000).
[45] Hearing record, *supra*, at 20 (testimony of Lieutenant Myers).
[46] Chris Hibbert, *What to do When They Ask for Your Social Security Number* (Apr. 5, 1997) **http://www.faqs.org/** (Internet FAQ Consortium, *Internet FAQ Archives,* Usenet FAQs, Filename privacy/ssn-faq).

card, a tax exempt card, a gun owner's permit, and a resident activity coordinator certificate.

Even more alarming is the availability online of government agency credentials. Lieutenant Myers noted that most law enforcement credentials are "much easier to copy and counterfeit than driver's licenses." Unlike driver's licenses, most law enforcement credentials are "merely a picture stuck on a card and laminated."[47] The Subcommittee learned that in general, law enforcement credentials frequently use fewer security features than do State driver's licenses.

Several investigations have shown the ease with which such technology can be used to gain unauthorized access to a variety of sensitive areas. This problem was highlighted at a House Judiciary Subcommittee hearing held on May 25, 2000,[48] for example, which detailed how investigators from the U.S. General Accounting Office (GAO) Office of Special Investigations (OSI) used credentials they had made using the method described above by Lieutenant Myers to gain easy access to 19 secure Federal sites and 2 commercial airports.[49] In a similar operation at certain sensitive Defense Department facilities in May 2001 commissioned by Senator Collins, GAO/OSI investigators penetrated the sites using easily-obtainable false identification—thus demonstrating their potentially catastrophic vulnerability to unauthorized access by criminals or terrorists.[50] GAO's findings in these multiple penetration tests demonstrate that, in addition to the lax security measures in place at Federal facilities and airports, the Internet and computer technology allow nearly anyone easily to create convincing identification cards and credentials.

Various reviews of the security of identification documents have long noted the problems caused by the variety of different identification documents used in the United States. Reverend Theodore Hesburgh, past chairman of the Select Commission on Immigration and Refuge Policy, once described the United States as a "document forgers" paradise."[51] According to one 1989 estimate, basic civil documents are issued by over 7,000 jurisdictions:

> "The lack of uniformity, uneven quality, and relaxed rules of issuance of many of these documents guarantees widespread abuse. Falsified or stolen vital statistics records become "breeder documents" for a chain of false documents that open the doors to highly prized entitlements—legal resident status for illegal aliens, social security, food stamps, unemployment compensation, and guaranteed student loans."[52]

---

[47] Hearing record, *supra*, at 13 and 22 (testimony of Lieutenant Myers).

[48] *See generally, Breaches of Security at Federal Agencies and Airports:* Hearings before the Subcommittee on Crime, House Committee on The Judiciary, 106th Cong., 2nd Sess. (May 25, 2000).

[49] *See* U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports,* GAO/T–OSI–00–10 (May 25, 2000) (statement of Robert H. Hast) [hereinafter "Hast statement"].

[50] This investigation demonstrated such a serious security vulnerability that the Defense Department classified the previously-unclassified GAO report at the SECRET level in the wake of the September 11, 2001 terrorist attacks upon New York City and Washington, D.C. For this reason, it is not possible to provide any more details of the operation here.

[51] David Simcox, *Secure Information: The Weak Link in Immigration Control* (May 1989) **http://www.npg.org/forms/secure—id.htm** (quoting Rev. Theodore Hesburgh).

[52] *Id.*

(c) *"Breeder" Documents*

The Subcommittee found various Internet sites that offer a variety of other types of identification documents or information that could be used to create other false identification documents. Several websites offer to provide false birth certificates, for example, which can be then completed to create a new identity or be used for identity theft. Sands cautioned his readers in *Fake ID by Mail and Modem,*

> "The smart use of a fake ID is as a stepping stone to a new identity with REAL documents. It may be necessary to use high quality fake ID in the interim to rent a mailing address or open a bank account, but the final goal should be to dispense with the fake ID as soon as possible." [53]

Birth certificates, when accepted as authentic, can thus be what are called "breeder" documents,[54] allowing the individual who creates a false birth certificate to obtain authentic identification documents from an authorized government agency. In one case reviewed by the Subcommittee, which is explained in further detail in Section III.B.(1), Thomas Seitz obtained a blank birth certificate from a website, completed the birth certificate with the biographical information of another person, and used it to obtain a valid identification card from the State of New Jersey. Seitz explained his reasons at the Subcommittee hearing:

> "[T]he birth certificate is sort of the key. That is the preferred document of identity that most agencies, DMV and other government agencies, like to see. That, coupled with a second form, the W–2, enabled me to go to the New Jersey Department of Motor Vehicles and present those documents and they would, in turn give me the top document there, which is a genuine photo identification card." [55]

The Subcommittee found a number of templates for documents that are not typically issued by government organizations. These supporting identification documents, while not as universally accepted as a driver's license or birth certificate, allow individuals to obtain other legitimate identification documents. For example, an individual could use a false press pass or travel agent card to obtain a legitimate library card or account with a telephone company bearing the desired false identification. With those cards and account information, or the names and addresses that appear on bills, the individual could then obtain other more universally accepted forms of identification.

C. *Marketing Practices*

(1) *Message Boards and Chat Rooms*

Websites that offer false identification materials or documents market their products in a variety of ways. Some appeal to those seeking to change their identity. For example, the home page of

---

[53] Sands, *supra,* at 5.

[54] A breeder document is a document that can be used to obtain other valid forms of identification.

[55] Hearing record, *supra*, at 18 (testimony of Thomas W. Seitz); *see also id.* at Exhibit 12 (Seitz's fake birth certificate, W–2 form, and New Jersey identification card).

photoidcards.com offers customers the opportunity to "[d]isappear completely and start a new life!" Some sites tout the ability of the customer, using the materials supplied by the company, to create a wide variety of false identification materials. The site *fakeidzone.com* markets products to younger age groups, offering not only driver's licenses that would allow a juvenile to purchase alcohol, but also college transcripts and college diplomas.[56]

Internet discussion boards are a free and easy means of advertising both products and websites. A posting to the newsgroup "alt.2600.fake-id" by an operator of *phonyid.com,* referring to himself as "Cybersario," stated as follows:

> "Don't get ripped off ordering from those scam sites on the net, order from the company that has been selling online since 1994. *Phonyid.Com* has been featured in everything from High Times to ABC News. We supply the highest quality ids and we are the only site which offers actual State holograms. Before you purchase a fake id do a little research and you will find that *Phonyid.Com* is the most trustworthy supplier of fake ids on the net." [57]

The Subcommittee's investigation indicated that the operators of *Phonyid.com* posted as many as 600 messages on a variety of topics on news group message boards.[58] Messages posted on discussion boards reach large numbers of people quickly at minimal or no cost to the individual posting the message. Moreover, they target the desired audience of people who are Internet and computer savvy, and who may be interested in purchasing products online, or in using computer files such as templates.

Most of the individuals posting comments on the discussion boards sign their messages "anonymous" or make use of obvious pseudonyms. This allows individuals who sell false identification products to post messages purporting to be from their own "satisfied customers." Again using the "Cybersario" pseudonym, for example, the operators of *Phonyid.com* posted a number of messages in an attempt to assure potential buyers of their site's authenticity. In one instance, they posted a message saying "http//www/phonyid.com. The ids cost about $200.00 but they are realistic." [59] In another case, a posted message read:

> "Phonyid.com has really good ids. I use them when I need to pick up something when I am carding....has worked everytime [sic] so far. I think the price is high but what i use them for it doesn't really matter, i am getting rich anyway." [60]

In a third instance, a message was posted saying:

---

[56] *See* Hearing record, *supra,* at Exhibit 6 (Tim Catron, *Fake ID Zone* **http://www.digitalhideout.com/idkit.html**).

[57] *Forum alt.2600.fake-id* **http://www.deja.com/group/alt.2600.fake-id** (post by "Cybersario" on Dec. 15, 1999). This individual presented him/herself as a **Phonyid.com** customer.

[58] *See Domain Watch* (visited Dec. 17, 1999) **http://www.domainwatch.com** (posting history for **jccamh@aol.com**).

[59] *Forum alt.2600.fake-id* **http://www.deja.com/group/alt.private.investigator** (post by "Cybersario" on Aug. 25, 1999)

[60] *Forum alt.2600.fake-id* **http://www.deja.com/group/alt.2600.fake-id** (post by "Cybersario" on Nov. 30, 1999).

> "This site has the best id cards. Just got my id with hologram and it is the [deleted]. Cards only $150.00 but the hologram makes it worth it. I back these guys 100%." [61]

Using similar tactics, an individual styling himself "IMO" posted comments about several of the websites that had recently closed, again, possibly in an effort to boost the legitimacy of the sites:

> "Perhaps you people are unaware but all the major id sites have had their offices raid [sic] within the past few months. I would hold off on ordering for a little while, because the site you order from might be the next one busted. It started with Noveltyid4u.com, they got busted about 2½ months ago when the secret service raided them for making false government documents. Phonyid.com got busted about 2 months ago for making counterfeit driver's licenses and passports." [62]

The Subcommittee believes that the individual or group of individuals responsible for the above series of postings are the operators of the website. Furthermore, the Subcommittee placed orders with two websites, American Photo Company and *Noveltyid4u.com,* that the Subcommittee now believes were operated by a small group of individuals and may have been wholly fraudulent. The Subcommittee never received any product in return for the $283 it sent these two websites, nor, it suspects, did many other of these sites' would-be customers.

(2) *Deceptive Practices*

Website operators frequently use deceptive advertising to entice potential customers. Some make claims about the credentials of their employees, while others tout features of their cards that are likely to be untrue. Experience at a State department of motor vehicles (DMV) is one of the main lures the website operators employ. For example, *photoidcards.com,* a company based in Canada, claims that "all id cards are professionally designed by an ex-DMV staff," and that *photoidcards.com* has "25 years of experience working with DMV offices worldwide." [63] In fact, *photoidcards.com* includes commentary from the aforementioned alleged "former DMV" employee, who says of the *photoidcards.com* products that "the finish and design of virtually every aspect is outstanding." [64] Website operators tout the services of "former DMV" staff to attract customers, since many of the security features of State issued driver's licenses and the methods of making them are known only to DMV employees.

Website operators also claim that their products have certain hard-to-duplicate security features that are in high demand and lend authenticity to the counterfeit documents. For example, many websites boast that their fraudulent identification documents bear

---

[61] *Id.* (Post by "Cybersario" on Jan. 5, 2000).

[62] *Fakeidman's Discussion Forum* **http://network54.com/Hide?Forum** (re-post entitled "You were not scammed, THEY WERE BUSTED!!," posted on Apr. 3, 2000).

[63] Loren Marceau, *Home Page* (visited Dec. 12, 2000) **http://www.photoidcards.com.**

[64] Loren Marceau, *Frequently Asked Questions* (visited Feb. 4, 2000) **www.photoidcards.com/faq.html.**

holograms, working magnetic strips, and markings that appear under ultra violet light. Josh Dansereau of *Fakeids.org,* for example, promoted his products by stating on his home page that "all id's are digital id cards* with working mag stripes that really scan."[65] In his "Frequently Asked Questions" section, however, Dansereau admitted that the magnetic strips are not functional: "Do you have the credit card type of id with the magnetic stripe on the back? Yes, our ID's are the credit card style. The magnetic stripe on the back is for looks only, it does not really scan, it just makes the id more realistic."[66] Many States now encode a magnetic strip on the back of their driver's licenses with an individual's biographical information. This is of only limited utility, however, as most bars, banks and retail stores do not possess the equipment to test the authenticity of the magnetic strip on an identification card—and thus to tell a false identification with a non-functional strip from a real one.

Another prized security feature is the hologram. *IDnow.com,* for example, states that "the holograms we use are DMV issued meaning they will match exactly with an original ID."[67] *Theidshop.com* notes in the description of its PVC plastic identification documents:

> "The ID Shop is proud to be the first ID website to ever offer PVC plastic holographic ID's. These ID's are the highest quality novelty ID's money can buy. They also come with many added security options such as holograms."[68]

The difficult nature of obtaining realistic holograms is demonstrated by the high volume of postings on message boards concerning holograms. Most of these postings focus upon how to craft them or obtain them. Moreover, instructions on how to make a hologram are also frequently included on the identification kits that are marketed by many websites. (These instructions offer advice on what sort of reflective gold paint to buy, and how to craft stencils. Some suggest using gold eye shadow.)

Another deceptive marketing technique frequently employed by false identification website operators is to urge potential customers to order before the website is closed down by authorities—thus building market appeal upon the suggestion that the documents provided are so realistic that the site is operating illegally. In the advertising copy designed to promote his "New Identity Kit," for example, Jeremy Martinez stated that "We are revealing the secrets that they don't want you to know. Order now, before we are shut down by authorities."[69] Martinez offered products titled, "99 Ways to Disappear," and "Better Ways to Disappear."[70] Promaster Cards, a website based in the United Kingdom, similarly boasts about the illegality of its products, noting that "we continue to be a major headache to several DMV and Law Enforcement Agencies

---

[65] *See* Hearing record, *supra*, at Exhibit 30 (Josh Dansereau, *Home Page* (visited Jan. 3, 2000) **http://www.freehosting2.at.webjump.com/413a62646/fa/fakeids-org/gallery.htm**).

[66] Josh Dansereau, *Frequently Asked Questions* (visited Jan. 27, 2000) **http://www.freehosting2.at.webjump.com/413a62646/fa/fakeids-org/faqhelp.htm.**

[67] *Welcome to Idnow.com* (visited Jan. 3, 2000) **http://www.idnow.com/faq.html.**

[68] *See* Hearing record, Exhibit 31.

[69] Jeremy Martinez, *New Identity Kit* (visited Jan. 20, 2000) **www.vsub.com/newid./htm.** Martinez ultimately was shut down by the authorities.

[70] *Id.*

from around the world."[71] Promaster Cards also states that "we have been shut down several times by the FBI and Treasury Department under various forgery acts of US law."[72] Finally, the website boldly adds,

> "We are openly admitting that we are breaking State, Federal and several European law [sic] by providing ID that are exact replicas in every detail of the current IDs provided from the countries in our list."[73]

Statements of this type are obviously designed to entice people into buying products that appear so real that they are outlawed.[74] This, they clearly feel, is precisely what their customers seek.

(3) *Search Engine Placement and Keywords*

Many websites operators rely on the skillful use of keywords to place their websites high on search engine results lists. High search engine placement results in more visitors and, therefore, more customers. In his written response to a Subcommittee questionnaire, Jeremy Martinez explained the importance of using keywords effectively:

> "Since I am good at web promotion in the search engines, I am able to obtain prime spots in search engines, whereby surfers find me first and purchase from me instead of downloading [templates], from the free sites."[75]

Tim Beachum, operator of *bestfakeids.com,* reinforced this point during his Subcommittee deposition, noting that keywords affect "relevancy and a search engine ranking."[76] When asked which keywords he uses to market his site, Beachum suggested that he had found the words "Novelty Ids, Ids, Ids spelled with different cases, apostrophe-S, without the apostrophe-S, noveltyfakeIDs as one word, hyphenated, press pass" to be high-return keywords.

---

[71] *Promaster Cards* (visited Dec. 20, 1999) **http://members.xoom.it/—XOOM/driverid/page2.html.**

[72] *Id.*

[73] *See* Hearing record, *supra,* at Exhibit 13 (*About Promastercard* (visited Dec. 20, 1999) **http://members.xooPromasm.it/—XOOM/driverid/index.html).**

[74] On **bestfakeids.com/splash/splash.html**, Tim Beachum also used the ploy that the product price will soon rise: "The street price on our novelty fake id kit is $99.00, we sell the same kit online at a discount price of $39.97. If you order our kit before midnight [of a specific date] you only pay $29.97." The end-of-sale date changes automatically every day so that no matter when a would-be customer sees the site, the promotion will always appear to be *nearly* over.

[75] Hearing record, *supra*, at Exhibit 17 (Martinez questionnaire response, at 3 (Mar. 30, 2000)). *See Federal Trade Commission v. Jeremy Martinez, individually and d/b/a Info World,* Case No. 00–12701, Complaint for Injunctive and Other Relief (U.S. District Court for the Central District of California, Dec. 5, 2000); "Fake Ids" *City News Service* (May 18, 2001). Martinez's use of keywords, or "meta tags" to lure in potential customers did not go unnoticed by the Federal Trade Commission (FTC). In December 2000, the FTC filed a complaint in the U.S. District Court for the Central District of California alleging that Martinez deliberately marketed his website to consumers who were searching the Internet to find false identification documents. The complaint noted Martinez's use of such meta-tags as "illegal id," "fake id fraud," and "forging documents.

Pursuant to a May 2001 agreement approved by U.S. District Judge Christina A. Snyder to settle the FTC lawsuit, Martinez will pay $20,000. He also agreed permanently to shut down his website, which sold 45 days of access to fake ID templates for $29.99, and contained "high quality" templates for the creation of fake California, Georgia, Florida, Maine, Nevada, New Hampshire, New Jersey, Utah, Wisconsin, and New York driver's licenses. (Martinez's website also contained a birth certificate template, programs to generate bar codes—required in some States to authenticate driver's licenses—and a program to falsify Social Security numbers.)

[76] Subcommittee deposition of Timothy Beachum, at 11 (Apr. 5, 2000) ("Beachum deposition").

Beachum acknowledged under cross-examination that he also used the simple keyword "fake IDs."[77]

In fact, the Subcommittee examined the key words that several of the website operators used, and discovered that the use of the word "fake" and its variants appeared much more frequently than the word "novelty," despite the website operators' claims that their products were solely for "novelty," "entertainment," or "educational" purposes. Dansereau, for example, used approximately 22 keywords or phrases to advertise his website. The word "fake" (or a variant such as "false") appeared 12 times. Dansereau, in fact, did not use the word "novelty" to advertise his website at all.[78] Similarly, Brett Carreras, operator of *fakeid.net,* used approximately 37 keywords to market his website. The keyword "fake" or its variants appear 9 times in Carreras' usage, and the word "novelty" appears only twice.[79]

Tim Catron, the operator of *fakeidzone.com,* illustrated the effectiveness of keywords such as "fake" by making the results of his eXTReMe Tracking service available to the public.[80] While nearly 36 percent of the visitors to Catron's website used the keyword "fake" when searching for false identification on the Internet, less than two-tenths of one percent used the keyword "novelty."[81] Despite the fact that the advertising copy on these websites may contain the word "novelty," the websites clearly target those customers who are in search of authentic-looking false identification documents.

D. *Disclaimers Have Little or No Legal Impact*

(1) *Claims of Novelty*

Websites offering to produce false identification documents occasionally post disclaimers stating that the documents they sell are for "novelty" use only and should not be used for illegal purposes. Companies providing templates also frequently require users of their products to "agree" that they will not use the materials for illegal purposes. Sites may also require those accessing the information to waive liability against the company for any illegal acts, and to state that the individual using the site is not a law enforcement officer and will not use the material offered on the site as evidence for any charge of violating Federal, State, or local laws. One website providing templates seeks to avoid liability by asserting that the consumer is the one who actually produces the fraudulent document.[82]

---

[77] *Id.* at 141.

[78] Josh Dansereau, *Gallery* (visited Nov. 9, 1999) **http://www.fakeid1.com/gallery.htm.** Dansereau also used the keywords "False, Forging and Illegal" to advertise his website.

[79] Brett Carreras, *fakeid.net* (visited Dec. 21, 1999) www.fakeid.net/free.html. The keywords "forge" (or variants) and "phony" (or variants) are each used twice.

[80] *See Extreme Digital* (visited Jan. 24, 2000) **http://www.eXTRemeTracking.** Extreme Tracking is a service offered by Extreme Digital that tracks visitor traffic to a client's website. The information gathered includes the numbers of visitors, geographical and domain information about the visitors, and the keywords visitors used in a search engine to find the client's website. Catron made these records public in an attempt to demonstrate the profitability of his website to potential buyers in connection with his effort to sell the site through an online auction.

[81] *Id.*

[82] *See* Tim Beachum, *Best Fake ID's* (visited Mar. 13, 2000) **http://www.bestfakeids.com.**

Many websites purport to sell "novelty" or "fun" products despite marketing that undermines their claims. For example, Martinez offered a "New Identity Kit" that contains "[e]verything you need to create a new identity for fun!!" yet he encouraged Internet users to order "before we are shut down by the authorities."[83] On his website, *Bestfakeids.com,* Beachum continually referred to his product as a "Novelty fake id kit," but adds as a selling point: "Get a job as a Resident Activity Coordinator Guaranteed—good jobs are so hard to find and the system doesn't make it any easier."[84] In his Subcommittee deposition, Beachum noted that it was not his intention that customers use the certificate to get a job. He claimed that although "the whole site is a joke,"[85] he wanted his customers to think that the certificate "looked like the real thing."[86] Contradictory statements such as these undermine the website operators' contentions that they do not intend their products to be usable as authentic identification documents and clearly suggest that they wish to give regulators (and the Subcommittee) a rather different impression than would-be customers. Another example is Robert Sek, who operated "Theidshop," a producer of high-quality false identification documents "with many added security options such as holograms." Sek frequently referred to his products as "novelty Ids." However, he also stated that "Theidshop" was no longer accepting or processing orders from the State of Florida because of the statewide false identification program there.[87]

(2) *Disclaimers Do Not Discourage Sales*

Obviously, the disclaimers on these websites do nothing to prevent illegal use. Many websites have an initial page that states that users must read the disclaimer in its entirety and agree to its terms before entering the site. Frequently, however, very little of the fine print disclaimer is visible without extensive screen "scrolling," and nothing prevents users from simply hitting the "agree" button and proceeding directly to the main website pages without reading the disclaimer at all—although this is not uncommon with on-line software licensing and use agreements.

Many Internet users are conditioned to accept or agree to posted disclaimers without reading them, and may believe that disclaimers are of minimal importance. For example, university student Thana Barlee, who was arrested for making false identification documents for university classmates, noted in an interview with the Subcommittee that when he originally began searching the Internet for materials to use, he routinely ignored the disclaimers he read on the various false identification websites. Barlee added that he would see the disclaimers first, and then move to the main pages. Barlee told the Subcommittee that he was aware of the penalties associated with creating false identification but that, when he was making the documents, he paid no heed to them.[88] Seitz also recalled spotting a small disclaimer, and testified that

---

[83] Jeremy Martinez, *New Identity Kit* (visited Jan. 20, 2000) **www.vsub.com/newid./a.htm.**
[84] Beachum deposition, Exhibit 15.
[85] *Id.* at 30.
[86] *Id.* at 74.
[87] Robert Sek, *TheIDShop.com* (visited Dec. 21, 1999) **http://www.theidshop.com.**
[88] Subcommittee staff interview with Thana Barlee in Washington, D.C. (Mar. 23, 2000) (hereinafter "Barlee interview").

> "I frequently came across disclaimers on the individual sites stating, 'For novelty use only.' I cannot think of any reason why a statement like that would be there. It did not deter my actions in any way." [89]

Not only do website visitors attach little importance to the disclaimers, but some websites openly mock the disclaimers. The following is a disclaimer on the *drink.to/idtemps* website, operated by an individual identified as "Rustheriddler":

> "All information or files found on this site are for informational, entertainment, or educational purposes only. What you do with it is your responsibility and only yours, no one else! If you are a government employee or have anything to do with the government or law or anything at all, then you can't enter this site. You must be at least 3945 years old and may not be either male, female, or both. If you have purple skin, red hair with pink stripes, and wear pink leather pants made from whale skin then you may enter." [90]

Some operators reacted to Subcommittee scrutiny by quickly providing additional disclaimers. Until the Subcommittee contacted Beachum, for example, his website contained only the briefest of disclaimers:

> "Because our novelty fake id kit is distributed in a digital format we do not of [sic] refunds. Our kit is sold as is. All images found on this site is [sic] copyrighted, and can not be used by any other web site without the written consent of Best Fake ID's." [91]

After he first spoke with Subcommittee staff, however, Beachum quickly expanded his disclaimer to note that

> "[t]he information contained in this website is strictly for academic use alone. BEST FAKE ID's will bear no responsibility for any use otherwise. All information on this web site is for entertainment and educational purposes only." [92]

The Subcommittee found that both the website operators and the users attach very little importance to these disclaimers—unless, that is, they realize their activities are being studied by authorities.

(3) *Operators Use Disclaimers as a Shield*

Some website operators try to protect themselves from any sort of liability by using disclaimers on the materials they produce. Robert Sek, for example, shipped his false identification documents in a laminated and sealed pouch printed with the words "not a government document" in red ink on both sides. The document could be removed intact from this pouch easily and quickly. Sek's false identification cards also included a fine print disclaimer stating that the card was intended for novelty purposes only and that the

---

[89] Hearing record, *supra*, at 16 (testimony of Thomas Seitz).
[90] Rustheriddler, *Temps* (visited Dec. 1, 2000) **http://hammer.prohosting.com/idtemps/.**
[91] Tim Beachum, *Activity Coordinator Training Project* (visited Jan. 6, 2000) **http://www.Bestfakeids.com.**
[92] Tim Beachum, *Best Fake ID's* (visited Mar. 13, 2000) **http://www.bestfakeids.com.**

card is in no way affiliated or associated with any government entity—but this was printed in a nearly unreadable approximately 2-point font, and placed it in such a way as to resemble the boilerplate explanation of restrictions found on the backs of many genuine ID cards. Moreover, in some cases, the disclaimer may be present, yet remain undetected. As Lieutenant Myers testified at the hearing:

> "The word 'novelty' we find on a large percentage of identification cards that come off the Internet. It may be printed so small that you need a magnifying glass to read it, or it may be just part of the disclaimer that comes across. I know of no lawful purpose for someone to use a supposed novelty ID, and in hundreds and hundreds of cases that we have investigated, we find that the word 'novelty' is right on the license somewhere. It is just no one can take the time or has the ability to even detect it." [93]

Clearly, these types of illegible or easily removable disclaimers violate the terms set out in § 1738. As explained in Section I.(D) of this report, Federal law defines, for practical purposes, what a novelty identification card must look like. Under § 1738, any identification document bearing a birth date or age must "carry diagonally printed clearly and indelibly on both the front and back 'NOT A GOVERNMENT DOCUMENT' in capital letters in not less than 12-point type." [94] The term "identification document" is defined as "a type intended or commonly accepted for the purpose of identification of individuals and which is not issued by or under the authority of a government." [95] The statute provides for imposition of a penalty of up to 1 year's imprisonment for transporting in interstate or foreign commerce identification documents that do not meet these statutory requirements.[96] Because it was apparent that technology allowed some individuals to skirt this law, § 1738 was repealed by the Internet False Identification Act of 2000. Criminals can no longer hide behind the shield of such disclaimers.

Virtually all of the identification documents that the Subcommittee examined over the course of its investigation did not satisfy the above definition of novelty identification under Federal law. Accordingly, the unilateral efforts of the distributors of such products to characterize them as "novelty" identification in order to shield themselves from criminal liability are likely to be ineffective as a legal defense. Seitz, who used false identification documents to commit a crime, agreed that website operators post disclaimers merely in an attempt to protect themselves and mask their true intentions:

> "They are pretty much trying to cover themselves, in my opinion, because they do not necessarily go out of their way to say, go use this for an illegal purpose, but [by posting] the disclaimer, they are probably, in my opinion, trying to cover themselves. It does not discourage anyone." [97]

---

[93] Hearing record, *supra*, at 23 (testimony of Lieutenant Myers).
[94] 18 U.S.C. § 1738 (a)(1)–(2).
[95] *Id.* at § 1738(b).
[96] *See id.* at § 1738(a).
[97] Hearing record, *supra*, at 19 (testimony of Thomas Seitz).

To be sure, there are true novelty identification sites on the Internet.[98] The Subcommittee's investigation, however, did not focus upon such sites because of their obviously novelty nature. For example, a "Super Secret Agent" card or a "Backseat Driver's License" is unlikely to assist anyone in committing bank fraud. The products that these sites offer bear little, if any, resemblance to the *bona fide* documents on which they are based. The sites that the Subcommittee targeted, by contrast, promote their products as being virtual, if not exact, replicas of *bona fide* identification documents.

It is also worth noting that some false identification websites do not carry any disclaimers whatsoever.[99] The Subcommittee examined a number of such sites, but could not gain much information about the operators because, in large part, they appear to be located abroad. (As a result, the Subcommittee was unable to compel their compliance with a subpoena.) Other sites operating without disclaimers use anonymous e-mail and free web hosting services, which do not verify their customers' contact information. Many persons using such services submit false contact information, making it—as intended—more difficult to track down the true operators behind such websites. Nevertheless, it is noteworthy that some false identification sites made no effort to shield themselves from scrutiny by a false claim of novelty. (The fact that many such websites appeared to be located overseas also illustrates the wisdom of repealing § 1738, which clearly seems to have functioned principally to provide United States-based false identification sites with a patina of legality through the use of ostensible "novelty" disclaimers.)

(4) *Legal Challenges to Disclaimers*

Several Internet discussion boards that the Subcommittee reviewed included messages on "novelty" identification.[100] The Subcommittee found that assertions of "novelty" with regard to the type of websites the Subcommittee investigated are often understood to be thinly veiled attempts to hide the sites' true illicit nature. Clearly, the marketing of these websites is very much at odds with the disclaimers that they post. Tim Beachum's site was a prime example. Prior to the time the Subcommittee contacted Beachum, he had only a single disclaimer posted in fine print on his website. This disclaimer stood in stark contrast to his more general claim that, by purchasing his products, customers could "create fake ids so real that you could fool your own mother."[101] As noted above, it was only after the Subcommittee had contacted Beachum that he added a clearly worded and prominently displayed disclaimer. Nevertheless, even such prominent disclaimers would not insulate Beachum from liability even before the repeal of § 1738, because the birth certificate and driver's licenses that he

---

[98] *See e.g.,* Hearing record, *supra,* at Exhibit 23 (*Coolcards—Postcards from the Net* (visited Nov. 29, 2000) **http://www.coolcards.com**).

[99] *See e.g.,* Hearing record, Exhibit 3 (*Idsolution.com* (visited Jan. 4, 2000) **http://www.idsolution.com**).

[100] *See e.g.,* Hearing record, Exhibit 27 (*FakeID.NetDiscussion Board* **http://www.carreras.net/discus** (post by "Webhost" on Oct. 13, 1999).

[101] Tim Beachum, *Best Fake ID's* (visited Mar. 13, 2000) **http://www.bestfakeids.com.**

offered do not bear disclaimers within the parameters of the statute.

Law enforcement has investigated and prosecuted website operators who rely on these disclaimers. For example, State and Federal law enforcement officials have investigated at least two operators of Internet websites—Josh Dansereau [102] and Robert Sek [103]—despite lengthy and prominently displayed disclaimers on their sites and the presence of at least notional disclaimers on Sek's product and on the plastic pouches in which it was delivered. The U.S. Secret Service's investigation of Sek, which was conducted jointly with the Texas Alcoholic Beverage Control Board, resulted in the execution of search warrants at Sek's Austin residence on March 10, 2000. Dansereau was sentenced to a term of probation after pleading guilty to violating a Florida statute criminalizing the distribution of false identification documents.

Two of the website operators that the Subcommittee examined closely, Carreras and Catron, invoked their Fifth Amendment privilege against self-incrimination as the basis for refusing to answer any deposition or interrogatory questions. Both of these witnesses posted disclaimers on their websites similar to those Beachum utilized.

All in all, the Subcommittee considers the posting of these disclaimers to be a disingenuous and ineffective effort to conceal the true purpose of such websites—namely, to distribute false identification documents by taking advantage of the speed, relative anonymity, and enormous client base the Internet offers.

E. *Role of the Internet*

(1) *The Internet Allows Instantaneous and Anonymous Sales and Transfers of False Identification*

Before the use of the Internet for commerce, businesses were largely limited to customers who could contact them (or whom they could contact) in person, by telephone, or through the mail. This placed some practical limits upon the size of one's customer base and imposed some largely unavoidable capital investment requirements. The Internet, however, makes geographic boundaries and overhead costs largely insignificant. Particularly in conjunction with credit-card-based payment systems, a customer in a remote location in one part of the world may now purchase materials from a business in a remote location in another part of the world, provided that both parties have access to the Internet. Indeed, the customer may not necessarily ever even know where the business is located, or anything more about it than the address of its website and whatever information happens to have been posted there. (As the Subcommittee also found in trying to track down the operators of false identification websites, the Internet provides powerful means by which to hide information about site operators.)

Unfortunately, these developments have proven to be a great boon for the false identification business. When the product purchased over the Internet consists only of computer files such as a false identification template, for example, it can be delivered al-

[102] *See* Josh Dansereau, *Fake Id One* **http://wwwfakeidl.com.**
[103] *See* Robert Sek, *The ID Shop* **http://www.theidshop.com.**

most instantaneously, increasing the advantages of such transactions as compared to traditional methods of marketing and distribution. According to U.S. Secret Service Director Brian Stafford:

> "Most of the false identifications either come from * * * the template on the Internet or they actually come from true identities that are scanned and then desktop publishing is utilized and it is ultimately placed on the Internet, where, as you know, a button can be pushed and it can be sent anywhere in the world." [104]

Moreover, the quality of the product is not affected by this transmission. As Lieutenant Myers testified at the hearing, "The graphics that can be produced on the computer, they can be electronically transmitted to anyone in the world in that same quality." [105] (Use of such readily-obtainable templates, of course, is decidedly superior to traditional false-identification techniques, which may have involved such crude expedients as using a razor blade or other instrument to alter identification documents individually.) For businesses promoting false identification materials, and for customers seeking such products, the Internet also allows an almost instantaneous transaction. An individual who uses the Internet can locate and produce the desired false identification document in an amazingly short period of time. Thomas Seitz testified during the hearing that he found the templates and created the fraudulent birth certificates that he utilized in "a matter of minutes." [106]

Using the Internet thus enables operators to keep their costs and risks at a minimum, while offering a product of consistently high quality with unprecedented rapidity and efficiency. All in all, this has proven to be a business bonanza. In fact, Trent Sands wrote in *Fake ID by Mail and Modem* that:

> The Internet has breathed new life into the world of false identification. Many new companies are springing up to meet the needs of those who want documentation saying they are someone else. * * * The robust health of the mail-order and Internet identification business is in stark contrast to the situation of just a few years ago.[107]

Websites selling "memberships" or access to password protected information may acquire customers who purchase continuing memberships using credit cards that are billed monthly by a third party with the understanding that the website operator will provide new information or additional services through the website. One Website offering access only to "members" promised, "More Updates Coming Soon! More being added all the time!" [108] Such up-to-date information can be useful in circumstances where a State modifies the design of or adds security features to a driver's license.

Elimination of the distance barriers for transactions involving false identification materials presents new challenges for law en-

---

[104] Hearing record, *supra,* at 26 (testimony of Director Stafford).
[105] *Id.* at 20 (testimony of Lieutenant Myers).
[106] *Id.* at 18 (testimony of Thomas Seitz).
[107] Sands, *supra,* at 1.
[108] Jeremy Martinez, *Homepage* (visited Jan. 5, 2000) **newid.ultramailweb.com.**

forcement. Bruce Schneider, Chief Technology Officer at Counterpane Internet Security, observed, "The Net changes the nature of crime. * * * This is the death of distance: Crime is no longer based on proximity."[109] Law enforcement agencies in the United States face particular jurisdictional and other obstacles when criminal activity based in another country affects United States citizens. The Internet compounds these problems because of its ability to promote commerce and communication between distant locations, combined with the ability to conceal users' identities.

A report of the President's Working Group on Unlawful Conduct on the Internet described the jurisdictional problems facing law enforcement agencies seeking to investigate crimes committed using the Internet:

> "The challenge to law enforcement is identifying that location [of a computer] and deciding which laws apply to what conduct. The question is how sovereign nations can meaningfully enforce national laws and procedures on a global Internet. Inconsistent substantive criminal laws are only part of the problem, for investigative techniques are also controlled by national (or local) law. For example, law enforcement agencies must consider such issues as transborder execution of search warrants."[110]

Concealment of one's identity provides those engaging in criminal activities another tool to avoid detection by law enforcement. In a statement delivered to the Senate Judiciary Committee, a Justice Department official noted that a

> "fundamental issue facing law enforcement involves proving a criminal's identity in a networked environment. In all crimes—including cybercrimes—we must prove the defendant's guilt beyond a reasonable doubt, but global networks lack effective identification mechanisms. Indeed, individuals on the Internet can be anonymous, and even those individuals who identify themselves can adopt false identities by providing inaccurate biographical information and misleading screen names. Even if a criminal does not intentionally use anonymity as a shield, it is easy to see how difficult it could be for law enforcement to prove who was actually sitting at the keyboard and committing the illegal act. This is particularly true because identifiable physical attributes such as fingerprints, voices, or faces are absent from cyberspace, and there are few mechanisms for proving identity in an electronic environment."[111]

---

[109] "Foil the Hackers? A Security Maven Discusses the Impossible," *Business Week* (Mar. 6, 2000), at 32F–32J (interview of Bruce Schneider, Chief Technology Officer, Counterpane Internet Security Inc., San Jose, California).

[110] U.S. Department of Justice's, Report of the President's Working Group on Unlawful Conduct on the Internet, at 20 (Mar. 9, 2000).

[111] *Internet Crimes Affecting Consumers:* Hearings before the Subcommittee on Technology, Terrorism and Government Information of the Senate Judiciary Committee, 105th Congress, 1st Session (Mar. 19, 1997) (statement of Robert S. Litt, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice).

(2) *Website Operators Disguise Their Names and Locations*

The Subcommittee found that several websites use a variety of tactics to make it difficult for law enforcement to discover their identities. Most websites on the Internet use simple addresses, such as *yahoo.com,* that allow companies to be easily identified through Network Solutions, the company responsible for registering most commercial websites in the United States. Domain names are usually accompanied by registration information that is publically available. This information normally contains the name of the company or individuals registering the website, their address, telephone number, and e-mail address.

Some operators of websites that offer false identification materials cloak their identities by providing false or erroneous information when their domain name is registered. For example, one website offering false identification materials registered its domain name listing a fictitious address and telephone number in Mexico.[112] Other sites operate using free server space from a web host, usually placing advertisements on the screens of users of such pages. For example, one website offering false identification material, Promaster Cards,[113] uses a web hosting service called Xoom,[114] which prevents public identification of the company or persons responsible for the site through Network Solutions. Such actions make it more difficult for law enforcement to contact such companies about their activities and, if the operations are run from foreign countries, render apprehension even more difficult.

Companies or individuals may also use a series of different web hosts and e-mail addresses to remain hidden from detection, akin to moving the location of a business every few weeks. This practice would be impossible for conventional businesses with physical locations because the cost would be prohibitive. It is simple to accomplish, however, on the Internet. Lieutenant Myers testified that on many occasions he has shut down a website, only to find the same site reappear at a new web address: "these people will be right back, and we have found in many cases that we have even arrested people for [violations of false identification statutes], then we find them back on the Internet." [115]

Websites offering false identification materials also frequently use post office boxes or the address of a commercial mail-receiving agency to receive mail. Such addresses can be established using intermediaries, thus masking the identity as well as the location of the actual operator of the business. In addition, such addresses can be quickly changed, and the address change can be made on the web page in a matter of minutes, allowing website operators to avoid detection by law enforcement. This method of preserving anonymity works for customers as well. Trent Sands, in his book on false identification, advises his readers to "*[a]lways* use a mail-receiving service to order any document from a false ID vendor. Never use your real name when ordering documents. *Always* pay

---

[112] Network Solutions, *Registration of idsolution.com* (visited Dec. 12, 1999) **http://www.networksolutions.com.**

[113] *See* Hearing record, *supra,* at Exhibit 13.

[114] Xoom is owned by NBCi.com. Promaster Cards actually uses an Italian subsidiary of Xoom. *See* **http://members.xoom.it/—XOOM/driverid/index.html.**

[115] Hearing record, *supra,* at 22 (testimony of Lieutenant Myers).

by money order." He suggests that this safeguard will help protect the customer from law enforcement crackdowns on false identification manufacturers—which may lead to authorities' acquisition of the names of and contact information for illegal manufacturers' customers.[116]

Many operators of websites offering false identification materials use e-mail accounts that can be obtained anonymously, and thus hinder easy identification of the operator. An individual may obtain a virtually unlimited number of e-mail accounts from sources that are free, and may avoid detection by frequently changing e-mail accounts.

Persons using the Internet to distribute false identification documents often use computer technology and features unique to the Internet to protect their anonymity and avoid law enforcement. For instance, one individual posted a message on the discussion board at *fakeid.net,* advising those who manufacture counterfeit documents how to avoid detection:

> "Never work at home, if possible and you have the means, never work in your own State or sell to people in your own State. Keep moving. Work out of hotels, your car or an Apartment in another name. (Laptops essential) Encrypt. They don't really need hard evidence, but you damn sure don't need to give them any.Keep nothing on hard drives and clean your free space often. * * * Keep business dealings separate. Ten people don't need to know you and each other. You should be known as a different name to each person. Have a new ID (a real one) on standby. Don't use it for [deleted] until you need it. Mandatory.Self explanatory. When you get out of jail you are now a convicted felon, life is now a [deleted]."[117]

As the Subcommittee has found with other Internet-related investigations, anonymity is a key element for many of the operators of websites conducting illegal activities. During this investigation, the Subcommittee found websites offering false identification documents that never stated the company's name, address, or telephone number.[118] Some operators of websites request customers to communicate only by e-mail[119] or require a purchase to be made by credit card over the Internet. Some companies intentionally locate outside of the United States or use mailing addresses in Canada or an overseas location in order to insulate themselves from investigation by law enforcement agencies in the United States. The web page of one company, Promaster Cards, stated as follows:

> "Already we have been shut down several times by the FBI and Treasury Department under various forgery acts of US law. * * * We have now moved our web site to the UK but continue to process orders for our clients from around the world from our studios in the New York area. In the

---

[116] Sands, *supra,* at 8 (emphasis in original).

[117] Hearing record, *supra,* at Exhibit 25 (*FakeIDNet Message Board* **http://www.carreras.net/discus** (post by "Risingson" on Oct. 13, 1999)) (original punctuation and spelling preserved).

[118] For example, the web page of **fakeid.net** has no company name, address, or phone number. *See* FakeID.Net **http://www.fakeid.net.**

[119] Hearing record, *supra,* at Exhibit 25.

> next few months we expect to be shut down again but we will bound back as always from another part of the net. Hopefully in the UK they will take a little bit longer to catch on." [120]

F. *Websites Offering False Identification Materials Facilitate Other Crimes*

While it is a crime in and of itself to manufacture and sell a counterfeit identification document, false identification documents can also be used to further engage in other illegal activities. Indeed, this is presumably the principal source of demand for such documents. When the Subcommittee commenced its investigation into the increasing availability of false identification and credentials over the Internet, it aimed to curb the use of false identification principally because of the host of other crimes ranging from underage drinking to credit card and bank fraud to identity theft that are facilitated by false identification. Senator Levin noted in his opening statement, for example, that false identification documents are:

> "often now being used to carry out improper or criminal activities—to obtain fraudulent loans, to evade taxes, to establish a new identity, to steal another individual's identity, to defraud Federal and State Governments, to misrepresent one's residence or place of birth or age for any variety of purposes." [121]

This sentiment was confirmed by Director Stafford, who noted that there is a false identification component to nearly every financial crimes arrest the Secret Service makes, including bank fraud, credit card fraud, telecommunications fraud and computer fraud.[122]

Bank fraud and identity theft may be more serious crimes than the manufacture of false identification, however, it is often the manufacture of phony identification that allows bank fraud or identity theft to occur. Moreover, as worrisome as crimes such as bank fraud and identity theft clearly are, in the wake of the terrorist atrocities of September 11, 2001, it now appears that the dangers of false identification are greater than most observers have imagined.

The Subcommittee found significant evidence of the criminal motivations of users of false identification from messages posted on various Internet discussion boards, a forum that has blossomed as the Internet itself has grown. For example, the following messages were exchanged on an Internet discussion board about false identification on March 15–16, 2000:

> "Who would pay 225$ for an Id with a holo[gram]??? thats just a waste of money and only losers would pay for it. And who would buy an id withouht a holo? only losers who just suck. Wizz is a good guy but if u wanna make money you should get authentic looking holos and not some crappy ones that are not part of the state and then mad people gonna buy. and whoever is stupid enough to buy an

[120] *Id.* at Exhibit 13.
[121] *Id.* at 4 (remarks of Senator Carl Levin).
[122] Hearing record, *supra,* at 26 (testimony of Director Stafford).

> Id without a Holo then you're gonna be [deleted] cause u will get caught.
>
> Will
>
> Will,
>
> I would have to disagree with you. When i can get them, i pay $300.00 for them with true holo's all the time. I have to have holo's on mine. Just to give you an idea, i am closer to being 40 years old than being 21 years old. So I am not using them to buy alcohol or get into clubs. I am using them at banks.(they have to pass the book check) So to pay $300.00 for one that looks exact is a no brainer. I would feel more comfortable paying $300.00 for a quality one, then trying to save myself some money by buying one for $25.00 and get nailed. This is one of those things that i truly believe that you get what you pay for. I do agree with you regarding the holo's though, if they are not the correct ones for that State then don't even bother putting them on, you will end up getting your [deleted] thrown in jail.
>
> —Ed" [123]

The Subcommittee discovered the following posting on a website containing a discussion boards that center on false identification materials:

> "+++URGENT+++
>
> "I need an american or canadian fake id, birth certificate and social security card that will get me from canada to the u.s. and will make it through immigration and border patrol
>
> —any State will work
>
> —high priority, money no problem, must be very well done and professional
>
> —please email me right away at [e-mail address deleted]" [124]

Another post by the web host of one site offering false identification materials stated as follows: "There are people out there that aren't 17 years old, snaking past that 80-year-old bar guy to snag a 40 oz. [beer]. There are people out there that craft stuff better than DMVs and more untraceable." [125] This same post advises others about tricks to avoid legal problems: "Use your language appropriately * * * integrate words like "novelty", "educational" and "informational" as often as possible." [126] Such users are clearly anticipating using their phony identification for a host of illegal activities, and are not intending to use their phony identification and

---

[123] *Id.*, Exhibit 26 (*Fakeidman Is ID List* **http://www.pages.eidosnet.co.uk/fakeidman/** (post by "Will" and "Ed" on Mar. 17, 2000)) (original punctuation and spelling preserved).
[124] *Fake ID Zone* **http://www.fakeidzone.com** (post by "tulip" on Feb. 21, 2000).
[125] Hearing record, *supra,* at Exhibit 27.
[126] *Id.*

credentials "for novelty purposes only," as the website operators suggest.

(1) *Identity Theft*

Identity theft is reported to be one of the fastest growing crimes in the United States, and led to the introduction of S. 1399, the Identity Theft Prevention Act of 2001 by Senators Feinstein, Shelby, Corzine, Kyl, and Grassley in September 2001. Identity theft is possible without false identification documents, but it is much more difficult.

Individuals who seek to engage in identity theft may find the Internet a valuable tool. In addition to using the Internet to gain personal information about an individual whose identity they may wish to steal, the Internet facilitates identity theft through the production of quality counterfeit identification documents. According to Norman A. Willox, Jr., Chief Executive Officer of the National Fraud Center,

> "The computer and, more recently, the Internet have brought identity theft to a much more insidious level. They have allowed the identity thief to obtain personal identifiers of multiple persons quicker; to access higher quality fake identification tools (driver's licenses, birth certificates, social security cards, etc.) and, through e-commerce, to render the credit transaction completely impersonal. The potential harm caused by an identity thief using the Internet is exponential.[127]

Not only was Thomas Seitz, who testified at the hearing about his use of false identification to commit identity theft, able to gather information on his potential victims by searching the Internet, but he was also able to obtain online the false identity documents he needed to commit identity theft. Seitz testified that it was largely because he was able to find personal information about other people, as well as the means to create false identification, that he committed the criminal acts for which he has been convicted:

> "Although at first I did not have the intent to defraud anyone, I started searching the Internet again and determined that there were a large number of sites that offered the means to make false identification and the opportunity presented itself." [128]

In July 2000, the Subcommittee learned of a case in which an individual used false identification that he very likely obtained from website operator Robert Sek to perpetrate identity theft and a host of financial crimes. After finding a wallet belonging to Dr. Charles Glueck, Benito Castro used false identification in Glueck's name to commit bank fraud, credit card fraud, and insurance fraud, eventually racking up $35,000 in debt on ten credit cards that Castro obtained in Glueck's name. Castro told Louisiana State Police Lieutenant Kermit Smith, who investigated the crime, that after he bought the identification over the Internet, the seller offered him

[127] National Fraud Center, Inc. and Norman A. Willox, Jr., *White Paper: Identity Theft: Authentication As a Solution 5* (Mar. 16, 2000) (presented at National Summit on Identity Theft).
[128] Hearing record, *supra,* at 15 (testimony of Thomas Seitz).

a job as a sales representative. The Subcommittee examined Castro's fake identification and found it to be virtually identical to the one the Subcommittee bought undercover from Robert Sek, right down to the disclaimer-bearing plastic pouch in which the identification was packaged.[129]

Castro's document, like the Oklahoma identification document the Subcommittee obtained from Sek directly, was printed on stiff white plastic, and closely resembled in its design, coloring and fonts, a Louisiana driver's license. Again, like the Subcommittee's document, this false identification document omitted the words "driver's license" and included a fine print disclaimer on the back. On August 9, 2000, in the 19th Judicial District Court of Louisiana, Benito Castro pled guilty to 10 counts of identity theft, one count of theft, and one count of bank fraud.[130] Castro, who is the first man sentenced under Louisiana's 1999 Identity Theft law, is currently serving a 10-year term of incarceration at hard labor without possibility of parole at a Louisiana State correctional facility.[131]

(2) *Recent Terrorist Acts May Have Been Facilitated by False Identification*

The consequences of failing to curb the spread of false identification are grave indeed, and go potentially far beyond simply facilitating under-age drinking—in fact, evidence indicates that some associates of the Al Qaeda terrorist organization may have used false identification and immigration documents. False identification documents and credentials can enable criminals to gain unauthorized access to secure areas in airports and to open bank and credit card accounts under false identities in order to finance their activities. In addition, phony identification enables criminals to obtain *bona fide,* yet unsupported and unauthorized, identification documents such as driver's licenses. Their efforts to hide behind such false identities makes it much harder for law enforcement and intelligence officials to identify them.

One week after the horrific September 11 attacks, Federal agents arrested three men who may be associated with the terrorists' network on charges of possessing false identification. The identification documents, which are in the name of another individual alleged to be an associate of bin Laden who was arrested later, include a U.S. Immigration and Naturalization Service Form I–94 and a U.S. Immigration and Naturalization Service alien identification card (both of which have been confirmed as false by the U.S. Immigration and Naturalization Service), and a United States visa (which has been confirmed as false by a State Department Diplomatic Service agent). The documents, which the suspects told agents were false, also included a U.S. Social Security Administration card, and a "World Service Authority" passport.[132] In addition,

---

[129] For more information on the Subcommittee's undercover purchase, see Section III.A.(1)(c).

[130] *State of Louisiana v. Benito Castro,* Case No. 09–00–680 (Nineteenth Judicial District Court for the Parish of East Baton Rouge, State of Louisiana, Aug. 9, 2000) (Information). More specifically, Castro was convicted of 10 counts of identity theft under Louisiana Revised Statute 14:67.16(C)(1), one count of theft of over $500 under Louisiana Revised Statute 14:67(B)(1), and one count of bank fraud under Louisiana Revised Statute 14:71.1.

[131] Keith O'Brien, "Identity Thief Gets 10 Years in Jail" *Times Picayune* (Aug. 10, 2000).

[132] *See United States of America v. Ahmed Hannan,* Case No. 01–80778; *United States of America v. Karim Koubriti,* Case No. 01–80779; *United States of America v. Farouk Ali-Hamoud,*

two of the individuals are alleged to have obtained driver's licenses in both Ohio and Michigan, apparently using false supporting documents.

The FBI is investigating whether some of the terrorists who crashed American Airlines Flight 77 into the Pentagon obtained *bona fide* Virginia identification cards using false supporting documents, such as false sworn statements attesting to their Virginia residency.[133] In a case that was opened prior to September 11, 2001, investigators are looking into how approximately 20 individuals in seven States obtained licenses that permitted them to haul explosives and hazardous materials such as dynamite, gases, and toxic or radioactive waste. It is unclear what they may have intended to do using these credentials.[134]

(3) *Infiltration of Federal Facilities Using Phony Identification*

Shortly after the Subcommittee's hearing on false identification, the House Judiciary Subcommittee on Crime held a hearing on May 25, 2000, which detailed the results of a GAO undercover operation and underscored the Subcommittee's findings about the dangers posed by the widespread availability of false identification. GAO investigators from the Office of Special Investigations (OSI) were able to breach security at 21 of the most secure buildings in the United States, including the CIA, the FBI, and several airports by claiming that they were armed law enforcement officers. The investigators displayed phony law enforcement badges and phony credentials that they had crafted themselves using graphics software and images culled from Internet websites, and which bore little resemblance to the genuine articles. When the investigators presented themselves at security checkpoints, they were waved around metal detectors and were not screened.

In a similar operation at certain sensitive Defense Department facilities on May 10, 2001 commissioned by Senator Collins, GAO/OSI investigators penetrated the sites using easily-obtainable false identification—thus demonstrating their potentially catastrophic vulnerability to unauthorized access by criminals or terrorists.[135] Upon learning that OSI had confirmed the suspected vulnerability of these facilities, Senator Collins immediately contacted Deputy Defense Secretary Paul Wolfowitz to notify him of these problems so that the Department could promptly begin corrective action. Though such improvements are now underway, GAO's findings in these multiple penetration tests demonstrate that Internet and computer technologies allow nearly anyone easily to create dan-

---

Case No. 01–80780 (each in U.S. District Court, Eastern District of Michigan, Sept. 18, 2001) (affidavit of Special Agent Robert Pertuso in support of Criminal Complaints), and Tamar Lewin, "A Nation Challenged: The Charges: Accusations Against 93 Vary Widely," *New York Times* (Nov. 28, 2001), at B6. "World Service Authority" passports are not government-issued. *See* **www.worldservice.org.**

[133] Brooke A. Masters, "Hijackers Exploited DMV Loophole," *Washington Post* (Sept. 21, 2001), at A15, and Tamar Lewin, "A Nation Challenged: The Charges: Accusations Against 93 Vary Widely," *New York Times* (Nov. 28, 2001), at B6, and Matthew Barakat, "Fourth Person Charged With Helping Hijackers Gain Fake Ids," *Associated Press* (Oct. 25, 2001), and Alexandra R. Moses, "Attacks Investigation Points to Pocket of Terrorist Support," *Associated Press* (Nov. 17, 2001).

[134] John Mintz and Allan Lengel, "FBI Arrests Liquor Store Clerk," *Washington Post* (September 21, 2001) at A14.

[135] As noted above, this investigation demonstrated such a serious security vulnerability that the Defense Department classified the previously-unclassified GAO report at the SECRET level.

gerously convincing identification cards and credentials.[136] (This problem is compounded by the vast array of law enforcement identification cards currently in use.)

III. *Case Studies*

The pages that follow contain brief summaries of the evidence that the Subcommittee collected over the course of its 5-month investigation about specific websites that manufacture and market counterfeit identification documents. This report also includes a brief summary of two instances that the Subcommittee examined where criminals went online to obtain false identification materials to further other illegal behavior.

A. *The Sellers*

1. *Robert Sek: theidshop.com*

(a) *Business*

Robert Sek, of Austin, Texas, was born in 1979. In April 1998 Sek used the alias Arthur Biscay (a combination of his middle name and his parent's street address) to register the domain name theidshop.com.[137]

Sek told Lieutenant Myers that he owned approximately $30,000 worth of equipment which he used to manufacture false identification documents.[138] In March 2000, while executing a search warrant at Sek's Austin residence, authorities seized a computer, photographic quality printer, lamination machine, identification booklets, printed identification cards, customer orders for identification products, money orders,[139] and other evidence—including a Century United safe containing hologram film and approximately $16,000 in cash.[140]

Sek told Lieutenant Myers that he sold his products for approximately $50 each, and that he generated approximately $600,000 in revenue annually. In addition, Sek told Lieutenant Myers that he made approximately 1,000 false identification documents each month.[141] Indeed, after searching Sek's trash on January 19 and February 7, 2000, investigators retrieved approximately 300 envelopes addressed to the ID Shop.[142]

In addition, Sek told Lieutenant Myers that his operation was extensive, employing at least 17 sales representatives across the United States. In fact, Sek advertised for employees on the "job openings" page of his website, which stated that

> "if you are the type of person who likes easy money, then this job is for you. We currently have 70 sales reps all over the United States making salaries ranging from $200 to

---

[136] Hast statement, *supra.*
[137] *Network Solutions* **http://www.networksolutions.com/whois/.**
[138] Affidavit of Clarke Skoby, Special Agent, U.S. Secret Service, at 1 (Mar. 9, 2000) [hereinafter "First Skoby affidavit"].
[139] Affidavit of Clarke Skoby, Special Agent, U.S. Secret Service, at 1 (Mar. 13, 2000) [hereinafter "Second Skoby affidavit"].
[140] *In re A Black Century Fire Safe,* Case No. A–00–111M (W. D. Tex. Mar. 13, 2000) (affidavit of Special Agent Clarke Skoby submitted in support of application for search warrant).
[141] First Skoby affidavit, *supra,* at 1.
[142] *Id.* at 3–4.

> $2000 a WEEK. The majority of our current sales rep's [sic] are college or high [school] students." [143]

(b) *Products*

On his website, Sek advertised identification documents for the following States: Arizona, Arkansas, Colorado, Connecticut, Georgia, Hawaii, Kansas, Louisiana, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oklahoma, Oregon, Pennsylvania, South Dakota, Virginia, and Wyoming.[144] Customers had a choice of two types of identification cards: a PVC card which cost $100, with an optional hologram for an additional $20, or a 3M process card which cost $60. The PVC cards all bore State-specific backings, while the 3M Process cards all used an identical backing. (Sek did not offer holograms on the 3M Process cards.) [145]

(c) *Subcommittee Purchase*

During its investigation, the Subcommittee purchased undercover a phony Oklahoma driver's license from "The ID Shop" for $100, using a false name and the photograph of Subcommittee Investigator Kirk Walder. The fake license arrived approximately 3 weeks later in a plain white envelope with a return address of ID Enterprises, located at a postal mail box in Austin, Texas. The document itself appeared to be made of stiff, white plastic measuring 3⅜ by 2⅛ inches on which was printed the photograph of Investigator Walder, along with a virtually identical representation of an Oklahoma driver's license, including the State seal, but omitting the words "driver's license" on its face. The document arrived encased in a clear, flexible plastic pouch which was sealed on all four sides, but not physically attached to the document. The pouch measured 3 by 2½ inches. Lining the inside walls of the pouch were two clear plastic sheets on which were printed diagonally in red ink "NOT A GOVERNMENT DOCUMENT" in approximately 20-point type and in capital letters. Investigator Walder was able to remove the document from the pouch bearing this disclaimer, however, simply by snipping open the pouch with a pair of scissors. This removal process took no more than a few seconds.

(d) *Disclaimer*

As noted previously, Robert Sek took several calculated steps in an effort to insulate himself from criminal liability. As part of the ordering process, Sek's customers had to sign a contract stating that they

> "understand fully that this instrument (novelty ID) is not representative of any State government affiliation, either local, State, or Federal, and is not issued or endorsed by any State or Federal Government agencies or departments." [146]

---

[143] Robert Sek, *The ID Shop Job Openings* **http://www.theidshop.com.**

[144] First Skoby affidavit, *supra,* at 2.

[145] *See* Hearing record, *supra,* at Exhibit 31; Robert Sek, *The ID Shop* (visited Dec. 21, 1999) **http://www.theidshop.com/products.htm.**

[146] *See* Hearing record, *supra,* at Exhibit 24 (Robert Sek, *Ordering* (visited Jan. 27, 2000) **http://www.theidshop.com/ordering**).

Moreover, the customers had to promise "not [to] alter or deface the ID in any way (from its' [sic] original State when it was mailed***)." [147] In addition, as described above, Sek packaged his products in the laminated pouches described above bearing the "NOT A GOVERNMENT DOCUMENT" disclaimer. Sek also included a disclaimer in approximately 2-point type on the back of the identification cards themselves. This tiny disclaimer provided:

> "I, without reservation or restriction understand fully that this instrument is not representative of any government affiliation, either local or State, or Federal, and is not issued or endorsed by any State or Federal Government agencies or departments. I understand that this instrument's sole purpose is for novelty use only. I agree to accept complete responsibility for any fraudulent use of this instrument as states in the original agreement between myself and the manufacturer/vendor. The vendor does not provide any warranties of merchantability for a particular purpose of noninfringement. The vendor shall not be liable under any theory or for any damages suffered by the bearer of this instrument. I further attest and affirm that my signature on the front of this instrument serves as evidence that I, the bearer/purchase, agree to the aforementioned agreement in its entirety." [148]

Each of these purported safeguards was easily circumvented. The customer's promise to behave appropriately, of course, provided no guarantee that Sek's customers would not misuse his products—particularly since, as we have seen, the market for false identification is apparently based upon their value in facilitating illicit activity. As described above, the plastic pouch bearing the disclaimer was easily removed. In addition, the fine print disclaimer on the reverse side of the identification card is itself easily removable, perhaps by design, as a message posted on an Internet discussion board demonstrated:

> "OK, the IDShop sends their ID in a white envelope, exactly as they describe on their Web page. When you open this envelope, the ID has a laminated wrap, extending well over the edge of the ID. It also has printed, NOT A GOVERNMENT DOCUMENT printed across the lamination in Red. This slip is easy to remove with a scissors, and takes less than a minute. Next the ID itself has a paragraph on the back explaining how the ID is not a government document and cannot be used as such, etc. Now everybody is telling you that this is hard to get rid of, but let me tell you, from firsthand experience I simply took a tough eraser, one found on the back of a pencil would do fine, and rubbed it tightly against the words. After a few mins, the writing starts to fade and in less than 5 minutes the writing is completely gone." [149]

---

[147] *Id.*
[148] *Id.*
[149] *Id, supra,* at Exhibit 10.

2. *Brett Carreras: fakeid.net*

(a) *Business*

Brett Carreras, a graduate of Loyola College in Baltimore, Maryland, was born in 1978. The Subcommittee's investigation indicates that Carreras registered the domain name *fakeid.net* on July 28, 1998. At that time, John DeMayo, a self-professed pioneer in the Internet false identification business, began directing Internet users to Carreras' new site, as DeMayo claimed to be leaving the false identification business.[150] Carreras paid DeMayo a fee for every thus-referred customer who purchased a product from Carreras's site. In late December 1999 or early January 2000, Carreras bought an additional domain name, *fake-id.com,* from DeMayo for $10,000. DeMayo estimated that Carreras earned between $5,000 and $10,000 per month from the website *fakeid.net.* (DeMayo told the Subcommittee that *fake-id.com* was a popular site and that he had received between 50 and 100 e-mail messages each day before he sold the site to Carreras.)[151] Billing records obtained by the Subcommittee indicate that, between mid-October 1999 and mid-December 1999, Carreras received 621 orders at his *fakeid.net* website that generated roughly $8,239 in revenue.[152]

(b) *Products*

As a free service, *fakeid.net* offered low quality driver's license templates in a format compatible with Adobe® Photoshop®[153] for all 50 U.S. States. However, the site offered "premium" templates designed to be used with Adobe® Photoshop®, including an "ultimate" New Jersey license, an "ultimate" Maine license, as well as templates for Wisconsin, Utah, Ohio, Arizona, Connecticut, Michigan, Idaho, Iowa, Louisiana, New York, and the Canadian province of Saskatchewan. These "premium" templates[154] were available to members for a monthly fee payable by credit card of $14.95.[155]

After the Subcommittee contacted Carreras, he modified the site, advising visitors that the templates had been removed and that he would not answer questions about them. It appears that Carreras made this statement in an attempt to convince both the Subcommittee and law enforcement that the premium templates, which were the only revenue-earning portion of the website, had been removed and that the website was out of business. In fact, however, the templates were still accessible on the *fakeid.net* website through a different series of links for several more months, although many paying customers may have been unaware that the templates were still available. Following customer complaints post-

---

[150] Subcommittee staff telephone interview with John DeMayo (Mar. 30, 2000) [hereinafter "DeMayo interview"].

[151] *Id.*

[152] Letter from Paul Kraaijvanger, Co-founder/Director, and Matt Walker, Controller, Verotel, to Kirk Walder, Investigator, Senate Permanent Subcommittee on Investigations (Jan. 6, 1999), at 2.

[153] Adobe® Photoshop® is graphic design software that allows users to edit and create images. The software uses a system of layers, each containing a different portion of the image. Layers allow users to overlay one portion of an image over another; for example, a signature can overlay a photograph. Users can also remove or hide layers. Users are able to edit almost all aspects of an image, including color, size, and transparency, as well as add text.

[154] These templates are layered, and therefore, able to be manipulated relatively easily using software such as Adobe® Photoshop.®

[155] Brett Carreras, *States* (visited Dec. 9, 1999) **http://www.fakeid.net/states.**

ed on the *fakeid.net* message board,[156] Carreras posted information on the message board informing regular customers of this "back door" to the templates: "There are all types of members services availiable [sic] to users who paid and were not able to download the files. Go to members services, and click on all of the links. take care." [157]

(c) *Disclaimer*

Initial access to Carreras' website was through a page containing the following advisory: "For my protection, and yours, you MUST read the below disclaimer BEFORE entering. Thank You." The referenced disclaimer is in a small box, and the only readily visible portion of the text reads:

> "1. This page is to be used purely for reference/education/ novelty purposes.
> 2. I am at least 18 years of age, and realize that I am individually responsible for my actions.
> 3. I understand that the act of downloading information * * *." [158]

Although the viewer may scroll down the text to read it in its entirety, it is not necessary to do so in order to gain access to the rest of the website. Instead, the visitor may simply click on the following statement: "LET ME IN!" [159]

(d) *Related Websites*

In February 2000 the Subcommittee discovered that the *fakeid.net* web host was planning to introduce two new websites in the near future: *Illegalimmigrant.com* and *fake-id.com.* Both domain names are registered to Carreras. *Illegalimmigrant.com* would purportedly specialize in "identity documents such as passports, social security cards, green cards, SSN lists, generators, prove-it cards, resident alien cards, birth cirtificates [sic] . . . and many more!" [160] At *fake-id.com,* it was said,

> "professionals will create licenses from any State you choose, based on our custom-made templates, These will be the finest ID documents on the planet, and will be backed by the professionalism of FakeID.Net!" [161]

Notably, these ventures stand in sharp contrast to the information posted on the "frequently asked questions" page of *fakeid.net,* where it was claimed that

> "We do NOT sell IDs from this site, nor do we know of places which sell IDs. Be wary of any site that says you can buy an ID from them. No site on the internet is endorsed by this site, or recommended by this site's propri-

---

[156] *See e.g., Fake ID Net Message Board* **http://carreras.netldiscus** (post by "Anonymous" on Mar. 24, 2000; post by "Reaper" on Mar. 25, 2000).
[157] *Id.* (post by "Webhost" on Mar. 27, 2000).
[158] Brett Carreras, *FakeID.Net* (visited Dec. 17, 1999) **http://www.fakeid.net/intro.htm.**
[159] *Id.*
[160] Brett Carreras, *Power Point Presentation* (visited Feb. 15, 2000) **http://carreras.net/welcome.**
[161] *Id.*

> etors. Furthermore the proprietor of this site has NEVER created a fake and/or novelty ID." [162]

Carreras declined to answer the Subcommittee's questionnaire after invoking his Fifth Amendment privilege against self-incrimination. In addition, at his Subcommittee deposition, Carreras invoked the Fifth Amendment in response to every question except his name, date of birth, and current address.

(3) *Tim Beachum: bestfakeids.com*

(a) *Business*

Tim Beachum, who was born in 1969, registered *bestfakeids.com* on May 25, 1999, using the company name Executive Computer Designs, which is located in Virginia Beach, Virginia. As of May 19, 2000, the website was still active, but Beachum had changed some of the content. By November 2000, however, the website appeared to have been taken down.

On April 5, 2000, Beachum voluntarily submitted to a Subcommittee deposition. Beachum testified that he established *bestfakeids.com* with an unnamed friend after they had a discussion about websites that sell novelty identification documents.[163] Beachum had discovered that there were more than 100,000 webpages referring to the subject of false identification. Beachum opined that, if there were that many websites pertaining to false identification, there must be a market for the service.[164] Throughout his deposition, Beachum provided limited information and changed some of the answers he had previously provided to the Subcommittee during telephone interviews.

In addition to *bestfakeids.com,* Beachum owned ECD Inc., which he said offered "electronic information" and "marketing products," Payless Web Hosting, and Bulletproof Marketing, which Beachum said were not yet operational.[165] Beachum could or would not break down the approximate monthly income that he receives from each of his websites, although he estimated in his response to the Subcommittee's questionnaire that *bestfakeids.com* provided 90 percent of his website revenue.[166]

(b) *Products*

The home page of *bestfakeids.com* contained a smaller version of the same logo used by *fakeidzone.com.* The site promoted its sole product—online access to a "fake id kit"—as follows:

> "Novelty fake id's are quickly becoming a big business online. Although our competitors spend most of the time claiming to have the best fake id's, and slandering the competitions [sic] name. We have decided to take a different approach and let our product speak for itself. We sell 40+ kits a day—that's almost 3 times what any other fake id site sells. Here is why the all new and improved

---

[162] Brett Carreras, *Frequently Asked Questions* (visited Dec. 17, 1999) **http://www.fakeid.net/faq.htm.**

[163] Beachum deposition, *supra,* at 26.

[164] *Id.* at 44.

[165] Id. at 16–20; *see* ECD Inc. **http://www.ecdinc.com/mb/.**

[166] *See* Hearing record, *supra,* at Exhibit 17.

> "Best Fake ID's" site out sells the competition 3 to 1: We don't sell novelty fake ids we show you how to create your own using your home computer. We provide you with templates and step by step instructions on what you need to create fake ids so real you could fool your own mother. As a BONUS you will receive a super high quality birth certificate that can be printed in the privacy of your own home. You will be given access to download 50+ templates that you can use to create your own fake ids. Our templates consist of drivers license, gun license, back stage passes, and much more. As of 12/1/1999 our collection of templates has been totally updated. Templates are created and added upon your request! *(No other site on the Internet offers this service).* No shipping and handling . . . You will be given instant access to your fake id kit, and your bonus birth certificate as well as our online threaded message board." [167]

Beachum supplemented the copy cited above with numerous illustrations of his products, as well as lengthy testimonials, complete with photos, from what purported to be "satisfied customers."

(c) *Subcommittee Purchase*

The Subcommittee purchased undercover access to Beachum's "kit" on February 9, 2000. The kit consisted of several scanned State driver's licenses from various States; templates for driver's licenses from Wyoming, Alabama, and "Pureto [sic] Rico;" a press pass template; a blank birth certificate from Victory Memorial Hospital in Waukegan, Illinois; and two resident activity coordinator certificate files.[168] Despite the representation on his website, however, the kit did not contain a template for a gun license.

The driver's license templates allowed an individual to produce his own driver's license by filling in the blanks. The Subcommittee found that it would indeed be possible to produce credible driver's licenses from the templates on Beachum's site.

The press pass template included space for an individual's photograph and personal information. It also bore a bar code and a background reflecting the legend "American Press Association." [169] Beachum promoted the press pass on his website with testimonials from three "satisfied customers" who had supposedly created press passes for themselves using Beachum's template, and then used the passes to gain access to backstage areas at various events. Under questioning during his deposition, Beachum admitted that the testimonials were fictitious:

"Q: What is that?
A: It's a novelty testimonial page for the press pass.
Q: Okay. Are you familiar with the text?
A: Yes. Yes. It looks familiar.
Q: Is any of it true?
A: No.
Q: None of it's true?

[167] Beachum deposition, *supra,* at Exhibit 15.
[168] *See id.* at Exhibits 16–20.
[169] *See id.* at Ex's. 8–11.

A: No." [170]

Beachum also claimed during his deposition that the press pass template, like the other files in the kit, was not capable of producing a physical press pass because he had "pixelated" [171] the template so that when it was printed out, the image would be distorted. The following exchange is excerpted from his Subcommittee deposition:

"Q: Do you think it's possible for anyone to actually use that, your press pass, to get into a concert?
A: No. For a fact, no.
Q: Why not?
A: Well, especially when I printed it, it's too small. I mean, you can't manipulate that.
Q: That cannot be manipulated?
A: Not into a larger format, no.
Q: Again, why not?
A: It would become pixelated." [172]

Beachum's claims that the template would become useless if actually printed, however, were false: The Subcommittee was easily able to print a press pass that was not distorted.

The Subcommittee learned from officials at Victory Memorial Hospital in Waukegan, Illinois, that the birth certificate Beachum offered is an exact replica of a birth certificate format used by the hospital before 1990.[173] The birth certificate depicted a sketch of the hospital and calligraphic text preceding blanks for the infant's name, the doctor's name, and dates to be filled in by hand after printing the certificate. The kit included a text file which offered specific instructions on how best to replicate an authentic birth certificate from Victory Memorial Hospital, including the type of paper on which to print the certificate, and what types of gold seals to use. For example, the text notes that:

"* The Administrators [sic] name during the era this certificate was issued was Donald Wasson. The Attending Physician's name was W. M. Smith.
* Donald Wasson's signature is signed with a blue inked fountain pen.
* All ohter [sic] handwriting is done in black ink with a fine point pen (i.e. Bic).

* * *

"Now in case you missed it, to the left and right of the picture of the hospital, are BLACK INKED FOOTPRINTS OF AN INFANT. These foot prints of course are not on the

[170] *See id.* at 91–92.

[171] A pixel (from "picture element") is the basic unit of visual information on a computer display or in a computer image. The more pixels an image contains, the clearer the image will be, and the higher the resolution is said to be. Images that contain few pixels, and thus less visual information, tend to appear granulated when they are enlarged. Although Beachum never explained fully what he meant by "pixelated," the Subcommittee understood him to mean that he had lowered the resolution, and that the image would thus appear on screen, or in print, in a granulated manner when enlarged.

[172] Beachum deposition, *supra,* at Exhibits 86–88.

[173] *See* Hearing record, *supra,* at Exhibit 7a.

scan (get you [sic] own damn baby!). The foot prints each face inward toward the horizontal center of the document, and lie adjacent to either horizontal side of the picture of the hospital. Remeber [sic], the footprints face inward (as in heel near the edge of the document, with toes closest to the picture." [174]

Beachum testified that he intentionally corrupted the background of the birth certificate by adding a "digital watermark" [175] to the certificate file that would cause it to print in a distorted manner, which he claimed would prevent customers from actually using it. In the following dialogue excerpted from his Subcommittee deposition, Beachum explained this purported distortion process:

"Q: After receiving that certificate from that site, did you make any changes or alterations—
A: No.
Q: —to the certificate?
A: Yes, yes, yes. I digitally encrypted the background of the certificate.
Q: How did you do that?
A: I forget, but it's a plug-in from Photo Shop that does it.
Q: Why did you do that?
A: In case someone tried to increase the dpi, it would pixelate the picture, the image.
Q: And the purpose of causing the picture to be pixelated is what?
A: To keep someone from trying to pass it off as a real thing." [176]

In addition, Beachum testified that the certificate had been pixelated the entire time it was on his website:

"Q: So for the entire time that that file has been on your website and offered to customers on your website, it's had the distortion element you described?
A: Yes." [177]

The Subcommittee subsequently determined that Beachum's testimony was possibly perjurious, since the certificate files on the kit which the Subcommittee had purchased undercover *before* Beachum's deposition generated actual hard copy documents that did *not* bear a digital watermark. Computer experts consulted by the Subcommittee confirmed that the certificate files had not been altered in the fashion described by Beachum.

The kit included two activity coordinator certificate files, which Beachum testified that he created by digitally scanning the original certificates awarded to his mother.[178] One certificate appeared to be issued by Kent State University,[179] while the other was purport-

---

[174] Beachum deposition, *supra,* at Exhibit 7.
[175] A digital watermark is digital data embedded either visibly or invisibly into an image or other type of digital document (film, photograph, etc.) which is designed to make counterfeiting the document more difficult.
[176] *See* Beachum deposition, *supra,* at 78–79.
[177] *See id.*
[178] *Id.* at 48.
[179] *See* Hearing record, *supra,* at Exhibit 8a (Tim Beachum, *Kent State University Certificate*).

edly issued by the Ohio Health Care Association.[180] Both certificates bore blanks for the user to record the name of the person who had obtained the certificates, and the date on which the certificates had been issued. Beachum's site claimed that the completed certificates would enhance one's ability to obtain employment as an activity coordinator, which the site described as a person who plans activities for individuals in nursing homes or for pre-school children. The site claimed that, in order to obtain a genuine certificate, an individual must take a course costing "a thousand plus dollars."[181]

Despite these representations on his website, Beachum testified that the activity coordinator certificate files were for "novelty" purposes only. Beachum explained that the certificates were offered only in "thumbnail"[182] format, and could not be downloaded in their full sizes. In the following exchange, Beachum insisted that if a customer were to download and enlarge the certificates, they would be useless because they would be hopelessly distorted:

> "Q: Is it your testimony that those documents, Exhibits 3 and 4, then could not be made to look like authentic documents?
> A: No. No way they could be.
>
> * * *
>
> Q: Why not?
> A: I intentionally corrupted the background of all the documents so that they couldn't be used.
> Q: How did you corrupt the background of the documents?
> A: I put a watermark, what is called a digital watermark in the background to give the paper an intentional crinkle or wrinkled look.
> Q: So it is your testimony that is someone—well, maybe you could explain for me, if someone tried to print out these documents, what would happen?
> A: It would have a distorted look, like—the background of this has like a yellow tint to it and it's a real distorted look in the background. In my opinion, there's no way it would look authentic.
> Q: How long have you had that distortion on these products?
> A: Always."[183]

Despite these protestations, however, the Subcommittee successfully printed full-size certificates with the use of software such as Adobe® Photoshop®. Thus, it appears as if Beachum may have committed perjury during his deposition testimony in this respect as well.

---

[180] *See id.* at Exhibit 8b (Tim Beachum, *Ohio Resident Activity Coordinator Training Project Certificate of Attendance*).

[181] Beachum deposition, *supra,* at Exhibit 15.

[182] A thumbnail is a picture of a graphic image. Thumbnails do not contain enough pixels, or picture information, to be enlarged or altered without significant distortion. Thumbnails are only used to indicate what an image looks like, and are not layered templates as described earlier.

[183] *See* Beachum deposition, *supra,* at 70–71.

(d) *Disclaimer*

Until the Subcommittee contacted Beachum, his website contained only the briefest of disclaimers:

> "Because our novelty fake id kit is distributed in a digital format we do not of [sic] refunds. Our kit is sold as is. All images found on this site is [sic] copyrighted and can not be used by any other web site without the written consent of Best Fake ID's." [184]

After he first spoke with Subcommittee staff, Beachum expanded his disclaimer to include the following:

> "The information contained in this website is strictly for academic use alone. BEST FAKE ID'S will bear no responsibility for any use otherwise. All information on this web site is for entertainment and educational purposes only." [185]

(4) *Tim Catron: fakeidzone.com*

(a) *Business*

Tim Catron is a Kansas resident who registered the domain name *fakeidzone.com* on October 2, 1998, providing as contact information an address in the Philippines. At this website, Catron offered a kit on a CD–ROM that he called "Fake ID Kit Ver. 2.0." He told the Subcommitte that he was reselling this kit for Brett Carreras.[186] Catron also said that he had previously "partnered up" with Carreras, the operator of *fakeid.net,* and Tim Beachum, the operator of *bestfakeids.com,* but that he had recently ceased all contact with those individuals.[187] Catron sold the CD–ROM kit for between approximately $19.95 and $39.95, payable by cash or money order. For a 2-month period, however, Catron accepted payment by credit card. Billing records obtained by the Subcommittee from his credit card processor indicate that, from November 1999 to January 2000, Catron earned $12,250 from 652 transactions.[188]

(b) *Products*

The CD–ROM disk that Catron marketed on his website contained more than 100 templates for a wide variety of identification documents, including driver's licenses, Social Security cards, green cards, and high school and college diplomas and transcripts, as well as what Catron referred to as "novelty templates" for documents such as a concealed weapons permit.[189] Catron's kit also included "step by step instructions on what you need to create fake ids so real you could fool your own mother," [190] as well as instructions for making both "a fake drivers [sic] license" and a hologram for the

---

[184] *Id.* at Exhibit 11.
[185] *Id.* at Exhibit 12.
[186] Subcommittee staff telephone interview with Tim Catron (Mar. 23, 2000).
[187] *Id.*
[188] Letter from Paul Kraaijvanger, Co-founder/Director, and Matt Walker, Controller, Verotel, to Kirk Walder, Investigator, Senate Permanent Subcommittee on Investigations (Jan. 6, 1999), at 2.
[189] *See* Hearing record, Exhibit 6.
[190] *See id.*

driver's license.[191] In addition to such tools as a bar code generator and a Social Security number verifier, the kit included instructions on how to "get a New ID: Complete report shows you how to do this by adopting the identity of a deceased child or infant."[192] To complete the kit, Catron sold paper designed for printing diplomas and birth certificates.[193]

(c) *Disclaimer*

Catron posted the following disclaimer at the bottom of his home page, in fine print:

> "Although our fake id kit gives you step by step instructions along with templates on how to produce realistic looking fake drivers license, birth certificates, back stage passes, and much more. It is only meant to be a novelty item. Do not under any circumstances try to pass them for the real thing. That would be illegal."[194]

In addition, Catron referenced the above disclaimer on his order form, and requested that customers sign the order form as an acknowledgment that they had read and understood the disclaimer.

Despite his novelty claim in the disclaimer, Catron refused to answer the Subcommittee's questionnaire by invoking his Fifth Amendment privilege against self-incrimination. He also stated in an affidavit that he would invoke the Fifth Amendment in response to every question except his name and address if the Subcommittee chose to depose him.[195]

(d) *Other Online Activities*

In January 2000, Catron attempted to sell his two websites, *fakeidzone.com* and *fakeid.cc,*[196] through an online auction at an offering price of $5,000. He noted in the auction description that the winning bidder would receive the domain names as well as the graphics and designs for his sites. Catron explained that although the site had been very profitable, he had decided to sell it in order to dedicate time to other (unidentified) sites.[197] Although it is not clear whether Catron successfully sold the websites, it does appear that he is no longer the owner of the domain names.

(5) *Josh Dansereau: fake-ids.com*

(a) *Business*

Josh Dansereau is a resident of Tallahassee, Florida, who was born in 1979. He originally became involved in the false identification business after he created a fake driver's license for himself.[198] In mid-April 1999, Dansereau registered the domain names *fake-*

---

[191] Tim Catron, *Fake ID Zone* (visited Jan. 3, 2000) **http://www.digitalhideout.com/idkit.html.**

[192] *Id.*

[193] *See* Tim Catron, *Placing a Order* [sic] (visited Jan. 5, 2000) **http://www.digitalhideout.com/cashorder.html.**

[194] *See* Hearing record, Exhibit 6.

[195] *See id.* at Exhibit 18 (affidavit of Tim Catron, Apr. 21, 2000).

[196] Subcommittee staff was unable to find evidence that **fakeid.cc** was ever operational.

[197] *See* E-Bay **http://www.ebay.com** (description of auction item 244333201, posted Jan. 23, 2000).

[198] Subcommittee staff telephone interview with Joshua Dansereau (Apr. 4, 2000) [hereinafter "Second Dansereau interview"].

ids.com, fakeidshop.com, and *fakeids.org.* In mid-September 1999 he registered *fakeidone.com* and *fakeid1.com.*[199] Dansereau used these five websites, which were mirror sites containing the same information, in an effort to gain more website traffic.[200]

Dansereau began selling false identification documents from *fakeids.com* in June 1999. He sold approximately 10 to 12 false identification documents per week at a price of approximately $30 to $35 each.[201] Dansereau used a high speed computer and monitor, a state of the art card printer, and a scanner to manufacture these documents.[202] Dansereau told the Subcommittee that he had made a total of 100 to 200 false identification documents, and as many as 50 in one peak month alone. Dansereau added that he had earned a total of approximately $3,000 to $5,000.[203] Lieutenant Myers believes that Dansereau earned closer to $250,000 from his false identification operation, and noted in his testimony during the hearing that when his team searched Dansereau's home, they found 85 fake identification documents ready to be mailed to customers. Lieutenant Myers noted that these 85 phony identification documents represented approximately $7,000 in income for Dansereau.[204]

(b) *Products*

Dansereau offered driver's licenses from all U.S. States with the exception of Florida.[205] Lieutenant Myers described the cards as high quality and noted that, of the 85 false identification documents his office confiscated from Dansereau, many were for older adults from a variety of States, including Florida.[206] On his website, Dansereau described his products as

> "The best novelty fake ID's you can buy. When held up to real State ID's, it's hard to tell the difference! You can be any age you want and you can be whomever you want. If you're looking for the most realistic fake ID's you can buy that will pass the book test, you have come to the right place."[207]

Dansereau distinguished his false identification documents from that of his competitors by noting that "all of are [sic] ID's are the new plastic credit card style, they come with a working magnetic strip at no extra charge."[208] In the "Frequently Asked Questions" section of the website, however, Dansereau acknowledged that the

---

[199] *Network Solutions* **http://www.networksolutions.com/whois/;** *see also* Hearing record, Exhibit 17 (Dansereau Questionnaire Response, at 1 (undated; returned to Senate Permanent Subcommittee on Investigations, Mar. 27, 2000)).

[200] Second Dansereau interview, *supra.*

[201] David Myers, Draft Training Materials: Joshua Dansereau Case Report 3 (Nov. 12, 1999) (unpublished report on file with Florida Division of Alcoholic Beverages and Tobacco Fraudulent Identification Unit, Enforcement and Training) [hereinafter "Dansereau Case Report"].

[202] Dansereau Case Report, *supra,* at 3.

[203] Second Dansereau interview, *supra.*

[204] Hearing record, *supra,* at 15 (testimony of Lieutenant Myers).

[205] *See* Joshua Dansereau, *Gallery* (visited Jan. 3, 2000) **http://www.freehosting2.at.webjump.com/413a62646/fa/fakeids-org/gallery.htm.**

[206] Dansereau Case Report, *supra,* at 3.

[207] Joshua Dansereau, *Fake ID One Home Page* (visited Jan. 3, 2000) **http://www.freehosting2.at.webjump.com/413a62646/fa/fakeids-org/gallery.htm.**

[208] Joshua Dansereau, *Gallery* (visited Jan. 3, 2000) **http://www.freehosting2.at.webjump.com/413a62646/fa/fakeids-org/gallery.htm.**

magnetic strips were not actually functional.[209] Dansereau accepted cash and money orders for his products, and suggested that customers wishing to pay with cash "wrap the money in a couple pieces of paper or something."[210]

(c) *Disclaimer*

Dansereau posted a lengthy disclaimer in fine print on the doorway page of his websites. The disclaimer was the same as that which was posted on Robert Sek's website, *theidshop.com,* see Section III.A.(1)(d). In addition, Dansereau posted the following statement on his home page:

> "Note: we are not recommending the use of the novelty ids to purchase alcohol or tobacco. That is illegal. When you purchase a novelty id. You assume all responsibility for the misuse of the product."[211]

These disclaimers, however, did not prevent Dansereau's prosecution by the State of Florida.

(d) *Legal Situation*

On November 12, 1999, Dansereau was charged with a felony for violating a Florida State law prohibiting the falsification of identification cards or documents purporting to contain an applicant's age or date of birth.[212] Dansereau pled guilty of the felony charge and, pursuant to a pretrial intervention agreement,[213] was sentenced to serve a 6-month term of probation starting in January 2000. He also forfeited the equipment he used to manufacture the false identification documents.[214]

Dansereau told the Subcommittee that he voluntarily shut down his false identification websites in either January or February 2000,[215] although one site, *fakeid1.com,* appeared still to be functional as of April 2000. Dansereau swore in an affidavit to the Subcommittee that when he shut down his false identification websites, he began returning orders that he had received to potential customers without opening them.[216] On February 4, 2000, as part of the Subcommittee's undercover operation, however, the Subcommittee mailed to Dansereau an order for a fake Connecticut driver's license. Despite two e-mail messages sent to addresses posted on Dansereau's website inquiring about the order, the Subcommittee did not receive the card and the money has not been returned.

In July 2000, because the Florida Division of Alcoholic Beverages and Tobacco Fraudulent Identification Unit (Florida ABT) suspected that Dansereau was still involved in producing or promoting false identification documents, his probation was extended until

---

[209] Josh Dansereau, *Frequently Asked Questions* (visited Jan. 3, 2000) **http://www.freehosting2.at.webjump.com/462b02686/fa/fakeids-org/faqhelp.htm.**

[210] *Id.*

[211] Josh Dansereau, *Fake ID One Home Page* (visited Jan. 3, 2000) **http://www.freehosting2.at.webjump.com/413a62646/fa/fakeids-org/gallery.htm.**

[212] *See* Florida Stat. ch. 877.18.

[213] *See* Florida Stat. ch. 948.08.

[214] Dansereau Case Report, *supra,* at 4.

[215] Telephone Interview with Joshua Dansereau (Mar. 17, 2000) [hereinafter "First Dansereau interview"].

[216] *See* Hearing record, *supra,* at Exhibit 19 (affidavit of Joshua Dansereau, June 7, 2000).

August 2000. As part of its ongoing monitoring of false identification on the Internet, Florida ABT determined that Dansereau had not shut down *fakeid1.com,* despite his assurances to the Subcommittee. Florida ABT then found that Dansereau had continued cashing and depositing money orders and cashiers checks that he received from individuals wishing to purchase false identification from *fakeid1.com.* As a result, Dansereau was arrested and again charged with a felony for violating Florida's false identification statute in August 2000.[217] Dansereau pleaded no contest to one count of failure to comply with requirements for sale of identification on May 23, 2001.[218] He was sentenced to a 3-year term of probation, ordered to pay $808 in court costs, and sentenced to perform 15 days of county work.[219]

B. *The Buyers*

(1) *Thomas Seitz*

(a) *Legal Situation*

Thomas Seitz, born in 1977, is a resident of New Jersey. In April 1999 local police in New Jersey arrested Seitz on charges of theft by deception and presentation of false information after he purchased a car on credit using an assumed identity. After pleading guilty, he was convicted in New Jersey State court of one count of theft by deception, two counts of forgery, and one count of uttering forged instruments.[220] Seitz was sentenced to a 3-year State term of incarceration for these four felony convictions.[221] On February 22, 2000, Seitz entered a plea of guilty to one count of bank fraud in the U.S. District Court for the Middle District of Florida for the same conduct that gave rise to the State charge. In June 2000, Seitz was duly sentenced to a 7-month term of incarceration to be served concurrently with his New Jersey State sentence, followed by a 60-month term of supervised release.

(b) *Internet Activities*

In an interview with the Subcommittee, Seitz said that he is very experienced with computers and the Internet. Seitz added that he has been using computers since the sixth grade, that he has worked as a computer network engineer, and that he was certified in the use of Microsoft products.[222]

At the hearing, Seitz testified that he was looking at various websites and discovered that he could obtain the names and Social Security numbers of other people from the Internet. Seitz knew that bank, credit, and tax information is tied often to an individual's Social Security number,[223] and that this information that can

---

[217] Affidavit of Jeff Yonce, Special Agent, Florida Division of Alcoholic Beverages and Tobacco Fraudulent Identification Unit, at 1–2 (Aug. 16, 2000) [hereinafter "Yonce affidavit"].

[218] *See* Florida Stat. ch. 877.18.

[219] *Florida v. Joshua Dansereau,* Case No. 00–3279 (Florida 2nd Judicial Circuit Court, May 23, 2001), and telephone interview with Special Agent Jeff Yonce, Florida Division of Alcoholic Beverages and Tobacco Fraudulent Identification Unit (Dec. 1, 2000).

[220] *See* New Jersey Stat. ANN. §§ 2C:1a(2),(3).

[221] *See New Jersey v. Thomas W. Seitz,* Case No. 99–06–00613–1 (New Jersey Superior Court Law Division, Sept. 27, 1999).

[222] Subcommittee staff interview with Thomas Seitz at the Baker County Jail, Macclenny, Florida (Apr. 6, 2000) [hereinafter "Seitz interview"].

[223] Seitz interview, *supra.*

be put to many uses, including identity theft. Accordingly, he found names and Social Security numbers on the websites for Congress and the Securities and Exchange Commission (SEC). By using search engines on the congressional website, Seitz was able to access the *Congressional Record,* where he found names, Social Security numbers, and military branches and ranks of members of the United States military being considered for promotion.[224] Seitz also found names and Social Security numbers of many individuals in the quarterly reports of publicly traded companies on the SEC's website. He focused his information-gathering efforts on at least two individuals, Joseph A. Parisi and Richard D. Clasen, both of California. He obtained these individuals' addresses and telephone numbers through online directories.[225]

Seitz then used Internet search engines to obtain information on fake identification documents, including birth certificates, Social Security cards, and driver's license or identification cards. Seitz recalled to the Subcommittee that while he was searching for false identification materials that he could use in conjunction with the personal information he had collected on Clasen and Parisi, he visited one site that posed the question: "Do you need a new identity?" Seitz downloaded templates including a birth certificate template from three or four free sites. Although one website Seitz visited stated that its products were for novelty purposes only, and another posted a small disclaimer, Seitz testified that he ignored both statements. Indeed, he wondered why anyone would put such templates on the web in the first place except in order to facilitate precisely the sort of illegal uses the disclaimers purported to disclaim—and for which he himself sought access to them. Seitz could see, for instance, no legitimate "novelty" use for a false birth certificate.[226]

Seitz conducted these Internet searches at a local library in an effort to avoid detection. He told the Subcommittee that he knew that the Internet Protocol address of a computer that had been used to visit a particular website could be traced. He explained, however, that

> "I used the computer in a public library to conduct my search. Dozens of people use the computers there every day and they also do not necessarily keep logs of who is using the computer. I had no fear of detection as I was searching."[227]

Using the stolen personal identification data that he had obtained from the SEC website, Seitz submitted 14 fraudulent car loan applications to Nations Bank via the Internet, including applications in the names of Clasen and Parisi. Seitz sought to obtain fraudulently a total of $540,000 in loan proceeds, but he received

---

[224] Names, complete Social Security numbers, and military branch and rank information of United States military officers under consideration for promotion were available through the *Congressional Record* until 1995. Since 1996, most entries—and since 1997, apparently, *all* entries—have contained only the last four digits of the Social Security number in addition to name, rank, and military branch information.

[225] Seitz interview, *supra.*

[226] *Id., see also* Hearing record, *supra,* at 16 (testimony of Thomas Seitz).

[227] Hearing record, *supra,* at 19 (testimony of Thomas Seitz).

checks for only the two loans for which he had applied in the names of Parisi and Clasen.

(c) *Creating False Documents*

After the loans were approved, Seitz used his home computer to complete a fake New Jersey birth certificate template that he had obtained from the Internet using the library computer. He made two different birth certificates using the identities of Parisi and Clasen, printing them on heavy green paper, but omitting the raised seal that the certificates were supposed to contain. The entire process took approximately 30 minutes. Seitz also obtained blank W–2 forms from the Internal Revenues Service website, and completed these documents using the stolen identities.

Seitz then used the counterfeit birth certificate to obtain an identification card in Parisi's name at the New Jersey Department of Motor Vehicles (DMV). He chose to obtain an identification card instead of a driver's license because he knew that only two pieces of identification were required for an identification card, and that he would not, in applying for one, have to wait long or take a driving test. As he anticipated, the DMV issued Seitz an authorized identification card in Parisi's name very quickly: It took about 30 minutes. Seitz also told the Subcommittee that DMV did not examine the W–2 forms that he provided as additional support.[228]

Seitz attempted to use his false identification card in Parisi's name to buy a car at a dealership in North Brunswick, New Jersey, but was unsuccessful because the dealership required an actual driver's license in order to make a purchase. Because Seitz did not possess a driver's license in Parisi's name, he abandoned his attempt to buy a car at that dealership.[229] Instead, Seitz scanned his New Jersey license into a computer, and used a software program to change the identifying information to that of Richard Clasen. This process took approximately 30 minutes. Seitz did not laminate this card, but simply printed it and photocopied the printout.[230] Armed with this merely photocopied driver's license, Seitz went to a different car dealership, located in the Township of Old Bridge, New Jersey, and selected a new car to purchase. Seitz presented to the dealership a photocopy of his altered driver's license, and recited aloud the Social Security number of an individual residing in California that he had obtained from the Internet. The dealership employees did not ask to see his W–2 forms or his birth certificate.[231]

Seitz was thus able to buy a car and drive it off the dealership lot successfully because the dealership employees did not verify his documents immediately. Although Seitz applied for, and received loans from Nations Bank, he was also able to finance the car through the dealership itself at a lower interest rate. New Jersey police discovered Seitz's crime in less than 2 weeks, however, because the number that Seitz inserted into the phony driver's license he manufactured in Clasen's name did not match an actual

[228] Seitz interview, *supra.*
[229] *Id.*
[230] *Id.*
[231] *Id.*

New Jersey driver's license number.[232] As a result, Seitz's fraudulent scheme was exposed when the dealership submitted the phony license number to the DMV to obtain the vehicle's registration. State police apprehended Seitz shortly thereafter.

(2) *Thana Barlee*

(a) *Background*

Thana Barlee entered a community college in Maryland after he was expelled from George Washington University during his freshman year in 1999 for manufacturing and selling counterfeit Maine and New Jersey driver's licenses in his dormitory room.

(b) *Internet Activities*

Barlee initially decided to create false identification documents in September 1999, after he was turned away from a local nightclub because he was not old enough to gain admission. Upon his return to campus, he started searching the Internet and discovered a wealth of information and resources related to false identification materials. Barlee found free, layered templates and instructions on a website operated by an individual whom he recalled as "Mo Mann."[233] Using these templates and such materials as reflective paint, paper, and lamination packs that he bought for about $40 to $60 at an office supply store, Barlee was able to create a fake driver's license that same weekend. Although this first fake license was sufficiently realistic to enable him to purchase alcohol at a nearby liquor store, Barlee worked to perfect his techniques over the next few weeks. He already owned a functional printer, but with investment backing from several other students, he upgraded to a higher-quality $600 printer, and bought a lamination machine as well. Barlee also used the Internet to purchase additional supplies for his operation, such as gold ink for making holograms.[234]

Barlee initially manufactured New Jersey driver's licenses because the general consensus on Internet discussion boards was that New Jersey licenses were the easiest to duplicate. The first weekend that Barlee was in business he sold approximately 15 to 20 phony driver's licenses to fellow students. He charged $20 to $100 for each license; the price he charged depended upon such factors as whether he knew the buyer and how quickly the buyer wanted the license. Barlee decided to diversify his manufacturing operation to include Maine driver's licenses because he thought it would look suspicious for so many college students to present New Jersey driver's licenses to a bouncer at a night club. He chose to duplicate Maine licenses because, like New Jersey licenses, they then had a reputation for being among the easiest to replicate.[235] With only about 20 minutes of experimentation, Barlee produced a high quality Maine driver's license.[236]

Barlee told the Subcommittee that he would not have manufactured and sold false identification documents had it not been for the ease with which the Internet enabled him to do so. On the "Mo

---

[232] *Id.*
[233] *See* **http://yohello.freeyellow.com/index.html.**
[234] Barlee interview, *supra.*
[235] Maine has since changed the appearance of its driver's licenses.
[236] Barlee interview, *supra.*

Mann" website, he found templates he could use to manufacture phony driver's licenses; step-by-step instructions for how to make and improve the quality of false identification documents; and a list of materials that he would need. Barlee saw the disclaimers on the websites but ignored them because such disclaimers are commonplace on the Internet.[237]

C. *Referrals*

Following the hearing, the Subcommittee referred several of the individuals and websites it investigated to proper law enforcement agencies pursuant to Rule 19 of the Subcommittee's rules of procedure—which provides that when there is

> "reasonable cause to believe that a violation of law may have occurred, the Chairman and Ranking Minority Member by letter, or the Subcommittee by resolution, are authorized to report such violation to the proper State, local and/or Federal authorities."[238]

The individuals thus referred include Mike Burton, Josh Dansereau, and the operators of *NoveltyID4U.com* and *Phonyid.com*—all of whom accepted orders and payment from the Subcommittee yet did not deliver a product. In addition, it is the Subcommittee's opinion that the activities of other individuals, including Robert Sek, Brett Carreras, Tim Beachum, and Tim Catron, warrant further investigation by law enforcement, as these individuals may have violated United States law. The offenses these individuals may have committed range from violations of § 1028 to perjury and mail fraud.

Unfortunately, little has been done in terms of prosecutions, although Josh Dansereau's term of probation was extended after Florida law enforcement learned that he had continued cashing customers' checks, including the Subcommittee's. In addition, the Fond du Lac, Wisconsin Police Department retrieved the $75 that the Subcommittee had sent Mike Burton for a false driver's license, and fined Burton approximately $200. However, it appears that the law at the time that Brett Carreras, Tim Catron, Tim Beachum, Robert Sek, and other individuals were operating their websites was not sufficient to prosecute them. With the exception of Brett Carreras, the individuals appear to have closed their websites and moved on to different ventures.

During the course of the Subcommittee investigation of false identification websites and their operators, at least seven websites closed down, including *bestfakeids.com,*[239] *fakeidzone.com,*[240] *ultimate-id.com,*[241] *newid.ultramailweb.com,*[242] *noveltyid4u.com,*[243] the "Fakeidman" message board, and *promasteridcards.com.*[244] In fact,

---

[237] *Id.*

[238] *Rules of Procedure,* for the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs as Adopted (March 8, 2001), S. Prt. 107–16 (March 2001), at Rule 19.

[239] *Bestfakeids* (last visited Nov. 30, 2000) **http://www.bestfakeids.com.**

[240] *Fake ID Zone* (last visited Nov. 30, 2000) **http://wwwfakeidzon.com.**

[241] *Ultimate Id* (last visited Nov. 30, 2000) **http://www.ultimate-id.com.**

[242] *New Identity Kit* (last visited Nov. 30, 2000) **http://www.newid.ultramailweb.com.**

[243] *Novelty ID 4U* (last visited Dec. 10, 1999) **http://www.noveltyid4u.com.**

[244] *Fakeidman* (last visited Nov. 30, 2000) **http://pages.eidosnet.co.uk/fakeidman.**

hours after the hearing concluded, *Promasteridcards.com* posted the following message on its website:

> "PromasterCards Ltd creased [sic] trading following the outcome of the Senate Governmental Affairs Permanent Subcommittee on Investigations on: "False ID's and the Internet" [sic] Any orders will be "returned to sender" 19th May 2000." [245]

IV. *Conclusion*

A. *General Services Administration Smart Card Technology for Federal Facilities*

In response to the results of the Subcommittee's investigation, coupled with recent terrorist assaults on the United States by individuals whose acts, and the preparation therefor, may have been facilitated by false identification, and GAO's findings that detail the weaknesses of security measures at Federal facilities, the Subcommittee has begun exploring methods of providing identification that cannot be so readily counterfeited. This exploration led the Subcommittee to the General Services Administration (GSA), which is currently in the final stages of developing so-called "smart card" technology.

Smart cards are credit card sized cards that contain a microprocessor. This computer chip is able to store, retrieve and process a variety of information that may be used for security purposes, including identification, entrance to buildings, and access to computers. The smart card can allow use of a range of biometric measurements for identification purposes, including fingerprints, hand geometry, iris (eye) scan, face measurements, and voice verification. Once an individual has enrolled his or her features, they are stored in a template that may be verified when the individual presents himself or herself at a security checkpoint. Smart cards can be used for many military applications as well as Federal employment applications such as equipment tracking, training updates, medical information, and accounting functions, thus eliminating the need for many different cards or forms. Smart cards may contain magnetic stripes, bar codes, and digitized photos.

At the request of the Office of Management and Budget (OMB), GSA first began working on coordinating a government wide adoption of smart cards in 1996. President Clinton's Fiscal Year 1998 budget demonstrated the administration's intention that every Federal employee be able to use a single card for building access, travel, small purchases, and other purposes. At this time, OMB directed GSA to work with Federal agencies, including the Department of Treasury and the Department of Defense, to develop a smart card. The GSA team responsible for this project met with representatives from industry and government agencies, then began conducting a pilot program within GSA and other agencies. On May 19, 2000, GSA awarded a Common Access ID Contract worth a total of $1.5 billion over 10 years to five firms. Several Federal agencies have expressed interest in the smart card, including the Veterans Administration, the Department of State, and the

[245] *Promaster Cards* (last visited May 19, 2000) **http://www.promastidcards.mcmail.com.**

Department of Defense, which has stated that it intends to use smart card technology for both military and civilian identification purposes.

One of the smart card's main strengths is its government-wide interoperability. It is GSA's intention that the cards be accepted at any participating Federal facility, so that, for example, cards issued by the Department of Defense will be compatible with the security measures at the Department of State. This should eliminate much of the confusion and potential for counterfeiting that stems from the multitude of cards used by Federal agencies, which has been highlighted by GAO's recent undercover operations. GSA's smart card incorporates cryptographic and biometric technology to encode an individual's information in a computer chip.

B. *Law Enforcement's Response to Crimes Using False Identification*

It is impossible to quantify the criminal activities that have been committed using false identification documents obtained via the Internet. The Subcommittee met with officials from the FBI, the U.S. Secret Service, the Social Security Administration, and various State law enforcement agencies. These officials indicated that, when they encounter cases involving false identification documents, they usually do not investigate the source of the documents, and frequently do not prosecute the false-identity crime itself because they concentrate instead on the offense that resulted from the use of the counterfeit documents. Director Stafford acknowledged that investigating the source of false identification is not the Secret Service's primary tactic in curbing the use of false identification:

> "We do not monitor specifically for false identification. We feel that we prioritize and focus our investigations primarily on crimes that involve false identification, primarily our core violations. We feel that through prioritizing, through addressing large dollar amount, high-impact cases that affect our community, whether it be credit cards or bank fraud or bank loans, all of which possess some form of counterfeit or fraudulent identification, that we can make an impact even with our limited funding and resources in this area." [246]

Moreover, anecdotal evidence exists indicating that the Internet has become a significant source of the false identification documents that are used illegally. Lieutenant Myers estimated that about 30 percent of the fraudulent identification documents that he reviewed in 2000 had been created via the Internet.[247] This figure, he said, had risen from slightly less than 1 percent in 1998, and approximately 5 percent in 1999. In addition, Lieutenant Myers testified that he expects that 60 to 70 percent of the false identification documents that his office will seize in 2001 will have come from the Internet.[248] (This includes identification documents pro-

[246] *Id.*, at 27 (testimony of Director Stafford).

[247] Subcommittee staff interview with David Myers, Lead Fraud Investigator, Division of Alcoholic Beverages and Tobacco, State of Florida, in Jacksonville, Florida (Apr. 7, 2000) [hereinafter "Myers interview"].

[248] Hearing record, *supra,* at 20 (testimony of Lieutenant Myers).

duced by website operators and identification documents produced through files transmitted over the Internet.)

As shown by the case study of Thomas Seitz, explained in Section III.B.(1), individuals seeking false identification to further criminal activities are increasingly likely to use the Internet to obtain false identification documents. In fact, Seitz testified that were it not for the ease of the Internet, he may not have searched for another source of false identification, adding, "I do not know any other places to go to get fake identification as good as on the Internet." [249]

It is vital that law enforcement focus its attention on this serious and growing problem, and in particular make every effort to curb the manufacture and distribution of false identification documents because, as K. Lee Blalack, II, then-Chief Counsel and Staff Director of the Subcommittee, testified:

> "the distribution of these counterfeit identification materials is growing because of the expanding technology of the Internet. This new technology could very well result in a flood of phony identification documents and counterfeit credentials if steps are not taken to curb this emerging problem. It will be no easy task to maintain the integrity of the identification documents on which both the government and the private sector rely." [250]

C. *Implementing New Legislation*

It is the Subcommittee's hope that the Internet False Identification Prevention Act of 2000, as well the Subcommittee's hearing, will focus attention on this emerging problem. Indeed, focusing attention upon this industry can itself help impede its operations. Lieutenant Myers testified at the Subcommittee's hearing, for example, that

> "Probably the biggest impact that we have had on the Internet as I monitor it and have for many years is the work done by your own Subcommittee's investigators. They had a dramatic impact on those on the Internet. Not even knowing their investigation was going on, I could see that the activity on the Internet as it related to false ID was going through some changes." [251]

Welcome though it is, however, such dissuasion through scrutiny and public attention is far from enough. The Internet False Identification Prevention Act of 2000 should help arm law enforcement officials with the tools needed to curb the manufacture and distribution of false identification documents over the Internet. Diligent efforts by the U.S. law enforcement community to employ these tools are now needed. As then-Chairman Collins noted during the Subcommittee's hearing:

> "One of the troubling findings of this investigation is that law enforcement officials, perhaps understandably, have focused on the crime committed with the phony IDs, but

[249] *Id.* at 18 (testimony of Thomas Seitz).
[250] *Id.* at 12 (testimony of K. Lee Blalack, II).
[251] Hearing record, at 21–22 (testimony of Lieutenant Myers).

> if we could somehow crack down on the manufacture and marketing of those IDs, some of the subsequent crimes would never be committed." [252]

Through aggressive law enforcement activity, and continued Congressional attention and oversight, the Subcommittee hopes and anticipates that it will be possible dramatically to decrease the number of crimes committed using false documents.

The following Senators, who are Members of the Permanent Subcommittee on Investigations, have approved this report:

Carl Levin
Daniel K. Akaka
Richard J. Durbin
Robert G. Torricelli
Max Cleland
Thomas R. Carper
Jean Carnahan
Mark Dayton
Susan M. Collins
Ted Stevens
George V. Voinovich
Pete V. Domenici
Thad Cochran
Robert F. Bennett
Jim Bunning

Other Senators, who are Members of the Committee on Governmental Affairs, approving this report are:

Senator Lieberman
Fred Thompson

○

[252] Hearing record, at 27 (statement by Senator Collins).