AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 106–574

PHONY IDS AND CREDENTIALS VIA THE INTERNET: AN EMERGING PROBLEM

HEARING

BEFORE THE

PERMANENT
SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MAY 19, 2000

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
64–986 cc WASHINGTON : 2000

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

COMMITTEE ON GOVERNMENTAL AFFAIRS

FRED THOMPSON, Tennessee, *Chairman*

WILLIAM V. ROTH, Jr., Delaware
TED STEVENS, Alaska
SUSAN M. COLLINS, Maine
GEORGE V. VOINOVICH, Ohio
PETE V. DOMENICI, New Mexico
THAD COCHRAN, Mississippi
ARLEN SPECTER, Pennsylvania
JUDD GREGG, New Hampshire

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
ROBERT G. TORRICELLI, New Jersey
MAX CLELAND, Georgia
JOHN EDWARDS, North Carolina

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

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

SUSAN M. COLLINS, Maine, *Chairman*

WILLIAM V. ROTH, JR., Delaware
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
PETE V. DOMENICI, New Mexico
THAD COCHRAN, Mississippi
ARLEN SPECTER, Pennsylvania

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
MAX CLELAND, Georgia
JOHN EDWARDS, North Carolina

K. LEE BLALACK, II, *Chief Counsel and Staff Director*
LINDA J. GUSTITUS, *Minority Chief Counsel and Staff Director*
MARY D. ROBERTSON, *Chief Clerk*

CONTENTS

Opening statements: Page

Senator Collins 1
Senator Levin 4
Senator Akaka 5

WITNESSES

FRIDAY, MAY 19, 2000

K. Lee Blalack, II, Chief Counsel and Staff Director, Permanent Subcommittee on Investigations, Washington, DC 8
David C. Myers, Special Agent, Identification Fraud Coordinator, Division of Alcoholic Beverages and Tobacco, Department of Business and Professional Regulation, State of Florida, Jacksonville, Florida 13
Thomas W. Seitz, user of counterfeit identification documents obtained from the Internet, convicted felon currently awaiting sentencing in the U.S. District Court for the Middle District of Florida 15
Brian L. Stafford, Director, U.S. Secret Service, Washington, DC 24

ALPHABETICAL LIST OF WITNESSES

Blalack, K. Lee, II:
Testimony 8
Myers, David C.:
Testimony 13
Prepared statement 31
Seitz, Thomas W.:
Testimony 15
Prepared statement 36
Stafford, Brian L.:
Testimony 24
Prepared statement 38

EXHIBIT LIST

*May Be Found In The Files Of The Subcommittee

1. Identification and credential montage 47
2. Connecticut Driver's Licenses—one authentic, one fake 48
3. *idsolution.com* Web site 49
4. Template for State of Maine driver's license 51
5. K. Lee Blalack's fake driver's license prepared with template from State of Maine driver's license identified above in Exhibit 4 52
6. Tim Catron's *fakeidzone.com* home page 53

7a. Authentic *Victory Memorial Hospital* birth certificate 54
7b. Tim Beachum's *Victory Memorial Hospital* birth certificate 55
8a. Tim Beachum's *Kent State University Certificate* 56
8b. Tim Beachum's *Ohio Resident Activity Coordinator Training Project Certificate of Attendance* 57
9. Fake Oklahoma driver's license 58
10. *Mexican 311* E-mail 60
11. Powerpoint presentation of Special Agent David C. Myers, Identification Fraud Program Coordinator, Division of Alcoholic Beverages and Tobacco, Department of Business and Professional Regulation, State of Florida 61

Page

12. Thomas Seitz documents 89
13. Page from PromasterCards Web site 90
14. May 19 and 30, 2000 Internet postings of PromasterCards 91
15. *SEALED EXHIBIT:* Permanent Subcommittee on Investigations Deposition of Tim Beachum, April 5, 2000 ..... *
16. *SEALED EXHIBIT:* Permanent Subcommittee on Investigations Deposition of Brett Skye Carreras, April 13, 2000 ..... *
17. Questionnaire sent by Permanent Subcommittee on Investigations to various Web site operators and replies received from Tim Beachum, Tim Catron, Josh Dansereau, and Jeremy Martinez 93
18. Affidavit of Tim Catron 113
19. Affidavit of Josh Dansereau 115
20. Statement for the Record of the Federal Bureau of Investigation 117
21. Statement for the Record of the Social Security Administration 120
22. E-mail: "Authentic Confidential New ID's—Driver's License!!!" ..... *
23. *coolcards.com*: "CoolCards—Postcards from the Net" ..... *
24. *theidshop.com*: Order page terms and conditions ..... *
25. Message Board: Risingson "advice," 10/13/99 ..... *
26. Will & Ed E-mail correspondence re: technology ..... *
27. Message Board, Webhost posts, 10/13/99, re: use of words "novelty" and "educational" ..... *
28. *excite* Web search results for "fake id," 4/12/00 ..... *
29. *carreras.net: "Premium Files"* ..... *
30. *fakeidone.com*: Home Page ..... *
31. *theidshop.com*: "PVC Plastic Id's" ..... *

32a. *prestigious-images.com*: "'Official' College Diploma Template" ..... *

32b. Fake ID Zone Kits ..... *

33. *alt.2600.fake-id* message board, Webdiaster post, 3/22/00, re: Ohio templates ..... *

PHONY IDS AND CREDENTIALS VIA THE INTERNET: AN EMERGING PROBLEM

FRIDAY, MAY 19, 2000

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:33 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Susan Collins, Chairman of the Subcommittee, presiding.

Present: Senators Collins, Levin, and Akaka.

Staff Present: K. Lee Blalack, II, Chief Counsel and Staff Director; Mary D. Robertson, Chief Clerk; Kirk E. Walder, Investigator; Eileen M. Fisher, Investigator; Brian C. Jones, Investigator; Adam Thomas, Intern; Barbara Cohoon, Intern; Linda Gustitus, Minority Chief Counsel; Michael Handley, Congressional Fellow; Felicia Knight (Senator Collins); Blake Thompson and Brad Tennison (Senator Cochran); Karin Rodgers (Senator Specter); Nanci Langley (Senator Akaka); Marianne Upton, Jessica Porvas, and Elaine Paulionis (Senator Durbin).

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. The Subcommittee will come to order.

Today, the Permanent Subcommittee on Investigations will explore a new and disturbing trend, the use of the Internet to manufacture and market counterfeit identification documents and credentials. This hearing is the culmination of a 5-month investigation by the Subcommittee that examined more than 60 Web sites which either distributed fake identification documents or the computer templates that allow customers to manufacture authentic-looking IDs in the seclusion of their own homes.

The high quality of the counterfeit identification documents that can be obtained through the Internet is truly astounding. As you will see from Exhibit 1,[1] which is on the monitor, with very little difficulty, my staff was able to use Internet materials to manufacture convincing IDs that would allow me to pass as a member of the U.S. Army Reserves—I note that my staff made me an E–4, not a general—— [Laughter.]

Senator COLLINS [continuing]. As a reporter, as a student at Boston University, or as a licensed driver in virtually any State—Florida, Michigan, Wyoming, to name just a few of the identities that I could easily assume.

[1] See Exhibit 1 which appears in the Appendix on page 47.

During the past decade, government agencies have added numerous security features to identification documents, such as holograms and bar codes, to prevent such counterfeiting. Yet, the Internet sites that sell fake IDs appear to have kept pace by duplicating many of these security features.

Displayed on the monitor is a comparison between an authentic driver's license provided by the State of Connecticut on the top and a fake Connecticut license that was created using a template obtained from the Internet.[1] As you will see, just like the real Connecticut license, the fake with my picture on it includes a signature written over the picture and an adjacent shadow picture of the license holder. The State of Connecticut added both of these sophisticated security features in order to reduce counterfeiting.

Unfortunately, some Web sites sell fake IDs complete with State seals, holograms, and bar codes to replicate a license virtually indistinguishable from the real thing. Thus, technology now allows Internet site operators to copy authentic identification documents with an extraordinary level of sophistication and then mass produce those fraudulent documents for their customers.

These counterfeit identification 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.

The Web sites investigated by the Subcommittee offered a vast and varied product line, ranging from driver's licenses for virtually any State to military identification cards to Federal agency credentials, including those of the FBI and the CIA. Other sites offered to produce Social Security cards, birth certificates, diplomas, and press credentials.

Because this is a relatively new phenomenon, there are no good data on the size of this new Internet industry or the growth that it has experienced. The Subcommittee's investigation, however, found that some Web site operators have evidently made hundreds of thousands of dollars through the sale of phony identification documents and other bogus credentials. One Web site operator told a State law enforcement official that he sold approximately 1,000 fake IDs every month and generated about $600,000 in annual sales.

Many of these Web sites are by no means subtle in their advertising. As you can see from the posterboard,[2] a site called *idsolution.com* informs its customers that it is "the leading source for all your identification needs." It urges customers to click on the link for a new identity kit, which is described as a complete package that allows you to really become someone else.

When you click on the new identity kit, you are directed to another page of the Web site that offers five fraudulent identification documents for $125. The new identity kit includes an American or Canadian birth certificate, a FedEx employee identification card bearing the customer's photograph, complete with holograms and even a magnetic swipe, three bills from AT&T, TCI Cable, and a

[1] See Exhibit 2 which appears in the Appendix on page 48.
[2] See Exhibit 3 which appears in the Appendix on page 49.

utility, all of which includes the name and address supplied by the customer. The site even offers a guarantee that the authenticity of these documents will be unmistakable from their original counterparts.

Subcommittee investigators attempted to contact *idsolutions.com* in late January, but it did not respond to our request for information. *idsolutions.com* ceased to operate shortly thereafter and we believe that the owners of this Web site have now gone underground to evade our investigation.

This highlights one of the principal challenges presented by these Web sites. Unlike a business with a physical address, a Web site operator can simply shut down the site once they are discovered, disappear, and then return to the Internet sometime later under a completely different name, making the job of law enforcement officials all that much more difficult.

For the criminal who has just stolen someone's identity, these sites offer an attractive service. For a relatively low price, the crook can get a State's driver's license using the victim's name and date of birth but showing the criminal's photograph, or the thief can obtain a fraudulent birth certificate using the stolen identity, then fabricate some utility bills purporting to show his or her address, and then use these documents to trick the Department of Motor Vehicles into issuing a real driver's license.

Subcommittee staff examined several sites that sell templates which a criminal could use by downloading it onto his computer and using it to make fake IDs again and again. Each time, the criminal appropriates a new identity. Our investigation found that driver's licenses are the most commonly fabricated identification document. These fake driver's licenses appear to serve as gateway documents that allow criminals access to other bona fide identification materials.

Identity theft is a growing problem that these Internet sites encourage. Fake IDs, however, facilitate a broader array of criminal conduct. The Subcommittee's investigation found that some Internet sites were used to obtain counterfeit identification documents for the purpose of committing other crimes, ranging from the very serious offense such as bank fraud to the more prevalent problem of underage teenagers buying alcohol or gaining access to bars. And indeed, as the Director of the Secret Service will tell us later, a false ID is almost always an essential element in financial crimes.

The Internet is a revolutionary tool of commerce and communication that benefits us all, but many of the Internet's greatest attributes also further its use for criminal purposes. While the manufacture of false IDs by criminals is nothing new, the Internet allows those specializing in the sale of counterfeit identification to reach a far broader market of potential buyers than they ever could by standing on a street corner in the shady side of town. They can sell their products with virtual anonymity through the use of E-mail and free Web hosting services and by providing false information when registering their domain names.

Similarly, the Internet allows criminals to obtain fake IDs from the seclusion of their own homes, substantially diminishing the risk of apprehension that attends purchasing counterfeit documents on the street.

At today's hearing, the Subcommittee hopes to shed much needed light on the growing and alarming use of the Internet to manufacture and distribute false identification documents. We will hear from both State and Federal law enforcement officials, including the director of the U.S. Secret Service, which is one of the key law enforcement agencies responsible for enforcing Federal laws prohibiting the distribution of counterfeit IDs.

These witnesses will be joined by a convicted felon who used the Internet to obtain a fake birth certificate and the names and Social Security numbers of several individuals, I might add, from public government Web sites, and then produced documents to commit identity theft and bank fraud. I look forward to hearing from all of our witnesses today.

I would now like to call on the distinguished Ranking Minority Member, Senator Levin, for any comments he might have.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Madam Chairman, first, let me congratulate you for taking the initiative to bring the attention of the Subcommittee, the Congress, and the country to a growing problem, and that is the use of the Internet to obtain documents which can be used for improper purposes very, very easily and very widely.

Although most of us recognize the extraordinary, positive capabilities and potential of the Internet, we have also become increasingly aware of and concerned about the use of the Internet for unlawful purposes. The worldwide appeal of and the access to the Internet carries with it both tremendous benefits and real risks. While it enables us to bring useful, beneficial information to every part of the globe, it also allows anyone on any continent to bring offers of illegal activity directly into a person's home. Wherever there is a computer connected to the Internet, there is the possibility of and the opportunity for misconduct. We are just beginning to observe and understand all of the implications of global access, and the proliferation of sites that promote fake identification is one such example.

The range and accessibility of various false ID products using the Internet is extensive. Using generally available search engines, my staff got literally thousands of hits by searching the Internet under the term "fake identification." While recognizing many of these hits represent the same actual Web site, there are conservatively, as the Chairman said, dozens of readily accessible sites which are active in providing false identification over the Internet.

Documents from fake driver's licenses, Social Security cards, and birth certificates to false passports and law enforcement credentials, including Secret Service agent IDs, are all readily available by a click of the mouse. These false IDs can be used for benign purposes, such as playing a trick on a friend or a family member, but they can also be used and are more 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.

The Secret Service, the Social Security Administration, and other Federal agencies have an interest in addressing these activities. My own home State of Michigan has recently established a High Tech Crime Unit in the Attorney General's office in order to focus on this type of activity.

The sale and promotion of false identification is more than a few young people obtaining false IDs for the purpose of underage drinking. Selling false identification over the Internet is a serious matter and a growing problem. With continuing technological growth, it is going to grow further and faster unless the tools for enforcement and deterrence are brought to bear and unless any loopholes in the law are closed.

This hearing will allow us to understand better the problems so that we might begin to move toward some meaningful solutions, and again, I want to commend our Chairman for calling this hearing, for her initiative in investigating this matter, and I want to thank the PSI staff for the hard work in preparing for this hearing.

Senator COLLINS. Thank you, Senator Levin.

I am pleased to welcome Senator Akaka, who has joined us, for any opening remarks that he might have.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Madam Chair and Ranking Minority Member, Senator Levin, for calling attention to another significant Internet-related privacy concern. The manufacture and use of false identification is a growing and vastly underpublicized problem.

The number of commercial Web sites advertising the sale of templates for making fake IDs and official documents is really striking. It is little wonder that incidents of identity theft and associated fraud have skyrocketed, in recent years. With the proliferation of commercial online information brokers, virtually anyone with a computer and modem now has the ability to search and quickly retrieve a wide range of personal information about others. The ease of access to this vast store of information facilitates ID theft and fraud at a fairly sophisticated level, with high expectation of success and little fear of detection. It is surprising that there are currently no laws regulating the publication of personal information in online databases.

Identification templates sold indiscriminately by Internet vendors includes driver's licenses for all 50 States, birth certificates, Social Security cards, military IDs, special agent and law enforcement IDs, professional licenses, college diplomas, and many others. A permit to carry a concealed weapon can even be obtained in this manner.

It is important to note that the possession and/or use of false identification for purposes of misrepresentation is a Federal crime and a crime in virtually every State. Yet, paradoxically, the sale and manufacture of IDs for the ostensible purpose of novelty use is significantly unrestricted.

I am proud to say that my State of Hawaii has been proactive in this area through enactment of tough laws. In Hawaii, the use of a fictitious name or having in one's possession a reproduction,

imitation, or facsimile of a driver's license is a crime punishable by a $1,000 fine and 1 year imprisonment.

Although I believe that statutory restrictions on information sharing should not be more restrictive than absolutely necessary to safeguard public and private interests, the unwarranted invasion of personal privacy posed by unregulated and indiscriminate information sharing is clearly unacceptable. I support ongoing efforts to create a comprehensive Federal policy guaranteeing individuals a right to control the collection and distribution of their personal information.

Is the practice of marketing and selling fake IDs a legitimate business practice consistent with constitutional protections that serve a greater societal good or a highly questionable practice that clearly facilitates fraud and other illegal practices? Well, I look forward to hearing the testimony of today's witnesses to help answer these questions.

Madam Chairman, I also have a longer statement that I would like to submit for the record, and thank you so much for this opportunity.

Senator COLLINS. Thank you, Senator Akaka. Your statement will be included in the hearing record.

[The prepared statement of Senator Akaka follows:]

PREPARED STATEMENT OF SENATOR DANIEL K. AKAKA

Thank you Chairman Collins and Ranking Minority Member Levin, for calling attention to yet another significant Internet related privacy concern. The manufacture and use of false identification is a growing and vastly under-publicized problem. The availability of high quality fake IDs via. the Internet is a small but important component of the much larger problem Congress has in protecting personal privacy, striking a proper balance of maintaining an open public record system, and ensuring freedom of speech and open commerce. It is undeniable that the computerization of publicly available data in recent years has heightened the importance and difficulty of balancing the divergent needs of access and privacy. Our private lives are now exposed in ways we never could have anticipated. I support the President's recently announced initiative to formulate comprehensive legislation to enhance financial and medical privacy, providing consumers the right of affirmative consent before sensitive information about them can be shared with others. I am pleased to note that Hawaii is in the forefront of enacting enhanced privacy legislation, and is one of the few states in the nation that now requires consumer consent prior to the release or exchange of their private insurance information.

The issue of privacy has not escaped public attention. Last fall the Wall Street Journal surveyed its subscribers about the most serious issue facing America in the twenty-first century. The top concerns were not the economy, education, or illegal drugs, it was loss of personal privacy. In another poll, the American Association of Retired Persons (AARP) found an overwhelming majority (93 percent) believes that any personal information they give during a business transaction should remain the property of the consumer and not be shared with other businesses without the permission of the consumer.

The Internet has had a profound impact—both good and bad—on our quality of life. It has literally revolutionized the world, stimulated our incredibly robust economy in heretofore unimaginable ways, increased efficiency, lowered costs, added convenience, and will no doubt serve as a primary stimulus for future scientific and economic breakthroughs. Unfortunately, the dark side of the Internet serves as a counterbalance, to remind us that evolving technology can also serve to our detriment. The information industry has grown dramatically every year, and shows no sign of slowing down. The Internet has the capacity to be the most effective data-collector known to man. The privacy problem is therefore likely to become more acute as more and more sensitive insurance and medical information is collected and exchanged over the Net. Although I believe statutory restrictions on information sharing should not be more restrictive than absolutely necessary to safeguard public and private interests, the unwarranted invasion of personal privacy posed by un-

regulated and indiscriminate information sharing is clearly unacceptable. I support ongoing efforts to create a comprehensive federal policy guaranteeing individuals the right to control the collection and distribution of their personal information.

The number of commercial Web sites advertising the sale of templates for making fake or IDs and official documents is striking—it is little wonder the incidence of identity theft and associated fraud has skyrocketed. In recent years, with the proliferation of commercial "on-line" information brokers, virtually anyone with a computer and modem now has the ability to search and quickly retrieve a wide range of personal information about others, including: names; addresses; social security numbers; telephone numbers (published and unpublished); dates of birth; relative names and addresses; neighbor names and addresses; criminal records; civil records; tax liens; real estate holdings; bank account numbers and balances; stock holdings; credit card account numbers and individual credit card transactions; long distance phone records; cellular phone records; pager records; 800 number records; motor vehicle records; driving records; aircraft and water craft ownership; credit histories; medical histories; where you shop and what you buy. Indeed, the profile of an individual which can be compiled using information stored in databases can be so complete as to constitute a near complete invasion of privacy. The ease of access to this vast store of information facilitates ID theft and fraud, at a fairly sophisticated level, with a high expectation of success and little fear of detection. It is surprising that there are currently no laws regulating the publication of personal information in online databases

Identification templates sold indiscriminately by Internet vendors include drivers' licenses for all 50 states, birth certificates, social security cards, military IDs, Special Agent and Law enforcement IDs, professional licenses, permits to carry concealed weapons, college diplomas and many others. It is important to note that the possession and/or use of false identification for purposes of misrepresentation are a crime in virtually all states. In Hawaii for example, displaying, lending, use of a fictitious name, or possessing a reproduction, imitation, or facsimile of a driver's license is a crime punishable by a $1000.00 fine and one year imprisonment. Federal statutes also impose criminal penalties for the production and use of false identification in some instances. Yet paradoxically, the sale and manufacture of IDs for the ostensible purpose of "novelty use," is significantly unrestricted.

Although Internet vendors post disclaimers that the fake IDs they sell are for recreational purposes only, these disclaimers serve as little more than thinly veiled attempts to indemnify vendors from legal responsibility for the most likely use of such items, that is, to facilitate underage purchase of tobacco products and alcohol, and to provide the means and instrumentality of identity theft and fraud. A relative novice with ill intent can easily acquire realistic ID templates, obtain publically available information about anyone he chooses, and follow specific Web based "how to" instructions for manufacturing fake IDs in another persons name.

Congress and the administration have aggressively petitioned industry to change policies and practices found to be overly intrusive or harmful to consumers, and have enacted laws as necessary to close loop holes. It is important to note that the Federal Trade Commission (FTC) and Direct Marketing Association (DMA) has worked together to provide comprehensive on-line guidance and information regarding a wide range of consumer privacy concerns including identity theft. Nevertheless, the rapid evolution of technology and increased availability of public information often outpaces efforts by industry or government to predict problems or to react quickly and appropriately once problems surface. Public awareness and vigilance are key to ensuring individual privacy needs are met. We need to ask ourselves if the practice of marketing and selling fake IDs is a legitimate business practice, consistent with constitutional protections that serves a greater societal good, or a highly questionable practice that clearly facilitates fraud and other illegal practices. I look forward to hearing the testimony of today's witnesses to help answer these questions.

Senator COLLINS. We will also include in the hearing record written statements that we have received from the FBI and the Social Security Administration. Without objection, these statements will be included in the written hearing record.[1]

Our first witness this morning is Lee Blalack, the Subcommittee's Chief Counsel and Staff Director. His testimony will provide an overview of the Subcommittee's extensive investigation of the

[1] See Exhibits 20 and 21 which appear in the Appendix on pages 117 and 120.

Internet's role in the manufacture and marketing of counterfeit documents. I would note that the Subcommittee staff has worked very hard on this and I look forward to hearing Mr. Blalack's presentation.

Our second witness will be Special Agent David C. Myers, who is the Special Agent in Charge of the Identification Fraud Unit for the Florida Division of Alcoholic Beverages and Tobacco. Special Agent Myers is a 20-year law enforcement veteran who has also served as a felony investigator for the Florida Highway Patrol and as a city police officer. A certified expert in electronic interception, Special Agent Myers has been involved in hundreds of felony investigations of identification counterfeiting, including Internet identification sales and identity theft.

Our third witness on this panel this morning is Thomas Seitz. Mr. Seitz recently pleaded guilty to bank fraud and is awaiting sentencing in the U.S. District Court for the Middle District of Florida. Mr. Seitz was apprehended by law enforcement officials in New Jersey after he used false identification documents that he acquired on the Internet to illegally obtain checks for approximately $60,000 in connection with several fraudulent car loans.

Pursuant to Rule 6, all witnesses who testify before the Subcommittee are required to be sworn in, and at this time, I would ask that the witnesses please stand and raise their right hands.

Do you swear that the testimony you are about to give to the Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. BLALACK. I do.

Mr. MYERS. I do.

Mr. SEITZ. I do.

Senator COLLINS. We will be using a timing system today. Please be aware that approximately 1 minute before the red light comes on, you will see the lights change from green to orange, which will give you an opportunity to conclude your remarks. We are not going to be that strict on time today, but if you could try to keep within the allotted time, that would be helpful. Your written testimony will be included in the hearing record in its entirety.

Mr. Blalack, I will ask you to proceed.

TESTIMONY OF K. LEE BLALACK, II, CHIEF COUNSEL AND STAFF DIRECTOR, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, WASHINGTON, DC

Mr. BLALACK. Thank you, Chairman Collins, Senator Levin, Senator Akaka, and members of the Subcommittee. Last November, Chairman Collins instructed the Subcommittee staff to examine the availability of counterfeit identification documents and credentials on the Internet and the criminal uses to which such phony documents can be put. Over the last 5 months, Subcommittee staff have devoted hundreds of hours to surfing the Internet as part of an effort to understand this little known but growing cadre of Web sites that offer fake identification materials. In furtherance of the investigation, the Subcommittee issued 11 subpoenas for documents and depositions and interviewed over 40 witnesses. My testimony today will provide a brief summary of that investigation and its findings.

The Subcommittee staff began this inquiry by using Internet search engines to develop a list of Web sites that offer fake identification documents. After reviewing over 60 Web sites, we focused our investigative efforts on 15 sites that purported to sell fraudulent identification documents or the means for customers to create those documents themselves.

The Subcommittee staff then commenced an undercover operation in which we ordered—using the fictitious name "Keith Wilson"—products offered by several of these Web sites. Through these undercover purchases, the Subcommittee acquired several high-quality false identification products, including a counterfeit driver's license for the State of Oklahoma, templates that could be used to produce fake driver's licenses from numerous States, authentic-looking birth certificates, and documents that could be used to fabricate credentials for employment.

Based upon this undercover operation and information obtained from the Web sites of these companies, the Subcommittee staff narrowed its focus to three major operators of Web sites that manufacture and/or market phony IDs. The first site is fakeid.net, which is operated by Brett Carreras, a 21-year-old student at Loyola University in Baltimore, Maryland. Mr. Carreras started his site on July 28, 1998. His site offers top-quality templates or computer files that allow customers to manufacture their own fake identification documents.

For instance, this is a file from Mr. Carreras's site that depicts a template for a previous version of a driver's license from the State of Maine.[1] We found that someone with a computer can use this template to manufacture a counterfeit license that is of very high quality. Indeed, at my request, Subcommittee staff used Mr. Carreras's template to create this fake Maine driver's license bearing my picture and did so in only a few minutes.[2]

In return for computer access to these templates, Mr. Carreras charged his customers a monthly fee of $14.95. Billing records obtained by the Subcommittee indicate that in the 2 months between mid-October 1999 and mid-December 1999, Mr. Carreras received 621 orders and generated over $8,000 in sales revenue.

Earlier this year, Mr. Carreras announced that he intended to open two more Web sites called *illegalimmigrant.com* and *fakeid.com*. Mr. Carreras advertised *illegalimmigrant.com* as a site that would specialize in "identity documents, such as passports, Social Security cards, green cards, SSN lists, generators . . . resident alien cards, birth certificates, . . . and many more."

The Subcommittee staff was unable to obtain additional information about Mr. Carreras and his Web sites because he declined to respond to the Subcommittee's interrogatories after invoking his Fifth Amendment right against self-incrimination. Mr. Carreras also refused to answer any substantive questions at a Subcommittee deposition on the grounds of his Fifth Amendment rights.

The second site is *fakeidzone.com*, which began operations on October 2, 1998. It is operated by Tim Catron, who resides in Law-

[1] See Exhibit 4 which appears in the Appendix on page 51.
[2] See Exhibit 5 which appears in the Appendix on page 52.

rence, Kansas. Mr. Catron sells a computer disk that includes templates for various types of fraudulent identification documents. Mr. Catron charges from $19.95 to $39.95 for the disk. Billing records obtained by the Subcommittee indicate that over a 2-month period in late 1999, Mr. Catron received 652 orders and generated revenue of over $12,000.

As this page from Mr. Catron's site indicates,[1] the disk contains a fake ID kit that includes "college transcripts you customize, college diplomas, new birth certificates, green cards, Social Security cards, updated driver's licenses, plus more." The site adds that, "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 with Mr. Carreras, Mr. Catron refused to give deposition testimony to the Subcommittee after invoking his Fifth Amendment right against self-incrimination.

The third site is *bestfakeids.com*, which is operated by Tim Beachum, a resident of Virginia Beach, Virginia. According to the deposition testimony of Mr. Beachum, he purchased the materials for his site from Mr. Catron and began operations on May 25, 1999. Mr. Beachum charges $39.97 for essentially the same fake ID kit that is sold by Mr. Catron. Mr. Beachum estimates that in the 1 year that his site has been operational, he has sold over 1,100 kits and earned almost $28,000 from the site.

Not only does Mr. Beachum's site offer driver's licenses, but he sells a birth certificate from an actual hospital in Waukegan, Illinois. During his deposition, Mr. Beachum claimed that he modified the birth certificate so that it would be distinguishable from the real certificate issued by the hospital. Subcommittee staff contacted Victory Memorial Hospital in Waukegan and obtained a copy of a birth certificate that it issued prior to 1990. As these two exhibits show,[2] the phony birth certificate sold by Mr. Beachum, which is on the left, is virtually identical to the authentic birth certificate that the hospital formerly used on the right. Mr. Beachum also sold fake press passes that he promoted with fictitious testimonials from individuals who had purportedly used the credentials to gain access to restricted events, such as concerts.

The Internet offers many exciting opportunities for commerce but, as our investigation has shown, it can also offer inventive criminals more effective tools to engage in illegal conduct. After reviewing the activities and products of these Web sites, we believe that several general findings can be made.

First, many Internet sites offer a wide variety of phony identification documents and some of these sites offer extremely high-quality counterfeits that include security features such as holograms designed to make the documents appear authentic. In fact, most of these sites market their products by touting the ability of the fraudulent IDs to pass as authentic.

Second, this marketing strategy is inconsistent with the disclaimers posted on some Web sites which claim that the phony IDs are for "novelty" purposes only. For instance, Mr. Beachum's site

[1] See Exhibit 6 which appears in the Appendix on page 53.
[2] See Exhibits 7a. and 7b. which appear in the Appendix on pages 54 and 55.

offers these two Activity Coordinator Certificates, which were supposedly issued by Kent State University on the left and Ohio Health Care Association on the right.[1] At his Subcommittee deposition, Mr. Beachum testified that he never intended for his customers to actually use these certificates to get a job. Indeed, his site includes a disclaimer that states, "All information on this Web site is for entertainment and educational purposes only."

However, Mr. Beachum's marketing shows that he expects and even encourages his customers to pass off these phony documents as legitimate credentials. His Web site states as follows: "Receive access to authentic downloadable certification certificates to get you a job as an Activity Coordinator. Why should you pay $1,000 for a couple of certificates just to learn how to plan activities for individuals?"

And, just in case the customer is not sure how to use these fraudulent documents, Mr. Beachum gives them some helpful hints: "We have received tons of E-mail from people wanting documents that could help them get jobs. . . . When you use the following certificates to apply for a job, you should use them together. On the first blank line, place your full birth name. On the last line place the date that the certificate was issued. Make sure that the date is the same on both certificates."

We do not know whether anyone has used these certificates, but we do know that Mr. Beachum sold them for that purpose. His marketing vividly illustrates how many of these sites attempt to shield themselves from criminal liability through the use of disclaimers that are patently disingenuous efforts to mask their intent to sell illegal products.

We found that these Web site operators are quite ingenious in their efforts to evade the law. Exhibit 9,[2] Chairman Collins, is an Oklahoma counterfeit driver's license that we purchased in part of our undercover operation from a Web site known as *theidshop.com*. With your permission, Chairman Collins, I would like to enter this fake license into the hearing record and submit it to the Subcommittee for inspection.

Senator COLLINS. Without objection, it will be included.

This is an example of how these Web site operators get around the disclaimer, is that correct?

Mr. BLALACK. That is correct, Chairman Collins. As you can see, as required by Federal law, the document appears to have the words "Not a Government Document" printed diagonally in red ink across the front and back. But, as you can see, this disclaimer is easily removed by cutting the top portion of the lamination and simply removing the actual identification document and, hence, the disclaimer.

Senator COLLINS. So, in effect, this license is sold in a laminated document that has the required disclaimers on it, but all one has to do is to remove it from the plastic pouch——

Mr. BLALACK. That is exactly right.

Senator COLLINS [continuing]. And then the disclaimer is no longer appearing anywhere on the fake ID?

---

[1] See Exhibits 8a. and 8b. which appear in the Appendix on pages 56 and 57.
[2] See Exhibit 9 which appears in the Appendix on page 58.

Mr. BLALACK. That is exactly right, Chairman Collins. And if that was not simple enough for some people, there are even message boards like this one here, Exhibit 10,[1] that instruct customers how to remove the disclaimer. It says, "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 scissors, and takes less than a minute."

Incidentally, this site is operated by a young man named Robert Sek, who recently had his operation shut down by the Secret Service and Texas authorities. Law enforcement authorities seized from his apartment a computer, photographic quality printer, ID making machine, printed identification cards, and a safe containing holograms and approximately $25,000 in cash. Pending the criminal investigation, Mr. Sek refused—through his attorney—to discuss his activities with Subcommittee staff.

Our third finding is that the Internet has greatly facilitated the manufacture and sale of counterfeit identification documents by allowing sellers to mass market high-quality fake IDs with virtual anonymity. This has, in turn, presented significant obstacles to effective law enforcement.

Mr. Catron's Web site illustrates the challenges that these Internet sites present to law enforcement. When he registered his Web site on the Internet, he attempted to disguise his true location of his operation by listing an address and telephone number in the Philippines, and an E-mail address that appeared to originate from another small country in the South Pacific. We eventually discovered that Mr. Catron directed payments from his site to an address in Pittsburgh, Kansas. And, we finally obtained Mr. Catron's actual location in Lawrence, Kansas, after enlisting the U.S. Marshals Service to serve him with a subpoena.

Mr. Catron's tactics, including the use of private mail receiving agencies and multiple anonymous E-mail accounts, allowed him to market his products to a wide audience with very little overhead cost and minimal risk of criminal exposure.

Chairman Collins, in conclusion, our investigation found that a significant number of Web sites offer a wide range of counterfeit identification documents, and that some of these sites offer phony documents of shockingly high quality. Moreover, we found that the distribution of these counterfeit 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.

Chairman Collins, this concludes my prepared remarks. I would be pleased to answer any questions that you and the Subcommittee might have regarding the staff's investigation.

Senator COLLINS. Thank you.

---

[1] See Exhibit 10 which appears in the Appendix on page 60.

We will next hear from Mr. Myers, and I want to thank Mr. Myers for all of the assistance he has given the Subcommittee with our investigation. You may proceed with your testimony.

TESTIMONY OF DAVID C. MYERS,[1] SPECIAL AGENT, IDENTIFICATION FRAUD COORDINATOR, DIVISION OF ALCOHOLIC BEVERAGES AND TOBACCO, DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION, STATE OF FLORIDA, JACKSONVILLE, FLORIDA

Mr. MYERS. Thank you. The Florida Division of Alcoholic Beverages and Tobacco under the Florida Department of Business and Professional Regulation has established the Fraudulent Identification Enforcement Program. This program has been established to obtain the most current intelligence on counterfeit identification. Other duties include technical review of ID scanning equipment, enforcement of counterfeit identification operations, possession of false ID enforcement, counterfeit identification detection training for law enforcement, and investigation of Internet sites that sell false IDs.

In the past 12 months, our training has been conducted to over 96 local, State, and Federal law enforcement agencies. Eleven arrests were made for sales and manufacturing of counterfeit IDs, with 33 Internet sites removed from the Web. Our intelligence gathering and training is the key to successful enforcement.

Over the past 4 months, over 300 arrests were made by our agency for possession of false identification. During this time, over 5,000 counterfeit IDs were obtained, and as you can see, there is a very large problem.

These IDs were also, when the subjects were arrested, identified as purchased from the Internet. A large percentage of counterfeit IDs we seize were purchased from the Internet. With these high-quality identification cards, detection has become very difficult. Many counterfeiters have advised that the templates they use to create identification were received from the Internet. These counterfeit IDs were not only used to purchase alcohol and tobacco by underage persons, but may also be used in bank fraud and identity theft.

Internet sales of false identification has increased dramatically. Identification is available on the Internet for all 50 States and many government agencies. With the use of current technology, high-quality identification cards and driver's licenses can be produced with easily accessible equipment. These high-quality identification cards can be purchased by anyone, in any name, with any date of birth.

Our main concern is protection of the public, industry, and saving the lives of our young people. I will show you a segment from our training program.[2] This is a common site which sells counterfeit identification that operates behind the word "novelty." This is one site that was operated by Josh Dansereau, which sold thousands of false identification cards. Fake passports are also very

[1] The prepared statement of Mr. Myers appears in the Appendix on page 31.
[2] See Exhibit 11 which appears in the Appendix on page 61.

common and can be purchased off the Internet for virtually any country in the world.

Some sites, like this one, sell all the information that you need on software to assist you in generating your own identification within your own home.

This site offers helpful hints on how to create false identification, including templates, birth certificate information, and bar coding which is used as a security feature by most States with the issuance of a driver's license.

Fakeidzone sells a complete kit on how to create high-quality ID on your own home computer.

As you can see, this Canadian site even sells police and FBI identification.

Many Internet sales sites recruit high school and college students to sell identification on school campuses.

This site, theidshop, operated by Robert Sek, at one time was the most popular site on the Internet. It was a million-dollar business. Though the operator of the site was located in Texas, we were able to communicate with him through his attorneys and our attorneys to prevent his sales of false identification to people within the State of Florida.

This is a restricted chat page where people discuss new ways to create counterfeit identification and avoid police. You have to have a special password in order to get into this chat page.

Here are some samples of counterfeit IDs sold on the Internet. Arizona—note the license on the left. It is a true and original license. The counterfeit licenses are on the right. If you will note—some of the licenses even have the hologram that are used by the State of California to protect their security, as well as by Colorado and Florida. Even the exact type of plastic and magnetic strip that is embedded in the plastic are used on these counterfeits, representing Georgia and Indiana. As you can see, it is difficult to determine the counterfeit from the original. New York—even the exact same paper that the State of New York uses, which is unique, is used on these counterfeit identification documents.

This is a Michigan license that even has a working magnetic stripe. This is a security feature that many States use to keep the license known as an original. It is a very important feature. Some identification cards are so—the counterfeits are so accurate that we cannot tell whether they are counterfeit or original by looking at the face. We use the magnetic encoded information to determine whether or not the license is counterfeit or original. Now that we are finding some that have a counterfeit magnetic strip, it makes it very, very difficult for law enforcement to determine the counterfeit from the original.

Here are some samples of holograms found on the Internet. Holograms are a security feature used by most States to restrict the counterfeiting of identification documents.

Law enforcement depends on ID. Without proper ID, we cannot do our job. Here is an operation we raided in Miami Beach where thousands of IDs were made. The equipment you see is basically the same type and style, uses the same printing materials as those used by most motor vehicle departments. The Internet was the backbone of this operation. The subject operated two stations al-

most 24 hours a day to create identification cards making, not just IDs for government agencies, but also certain security passes for airports and passes to get into restricted areas on government locations.

This young man, Josh Dansereau, was operating three different Web sites selling false ID until his arrest by our agency. These are some examples of licenses that he produced. With just basic equipment, you can easily make a 6-figure salary. This is some of the equipment that was used by Mr. Dansereau, basically the same equipment that is in the average home. Here are 85 fake IDs ready to mail. These were in the home of Mr. Dansereau when we entered it. This equals approximately $7,000 of income in one mailing for Mr. Dansereau.

Identification is the backbone of society. Our office is always ready to answer any questions that you may have. Thank you.

Senator COLLINS. Thank you, Special Agent Myers.

Mr. Seitz, would you please proceed.

TESTIMONY OF THOMAS W. SEITZ,[1] USER OF COUNTERFEIT IDENTIFICATION DOCUMENTS OBTAINED FROM THE INTERNET; CONVICTED FELON CURRENTLY AWAITING SENTENCING IN THE U.S. DISTRICT COURT FOR THE MIDDLE DISTRICT OF FLORIDA

Mr. SEITZ. Thank you, Chairman Collins. My name is Thomas Seitz. I am originally a resident of the State of New Jersey. I am presently incarcerated at the Baker County Correctional Facility in Macclenny, Florida. I am 23 years old and I am currently serving a prison sentence imposed by the State of New Jersey after I was convicted and sentenced to 3 years for committing the crimes of theft by deception, forgery, and uttering a forged instrument. I have also plead guilty to bank fraud and I am awaiting sentencing by the U.S. District Court, Middle District of Florida.

I appreciate the opportunity to testify before the Subcommittee. I hope that I can show its members how relatively easy it is for someone to engage in obtaining information from the Internet, including such personal information such as Social Security numbers. Moreover, I hope to show how easy it is to craft phony identification using that information and obtain significant amounts of money with very little effort.

I consider myself to be fairly well versed in the use of computers. I worked with computers since the sixth grade and I was employed as a network engineer. I obtained via the Internet names, Social Security numbers, and addresses of people by accessing files maintained as public records on the Securities and Exchange Commission Web site. 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.

I used a computer at the library in Old Bridge, New Jersey, and accessed various Web sites that offered documents for downloading, including birth certificates and driver's licenses. Some were free, so I found one that offered a New Jersey birth certificate and I

[1] The prepared statement of Mr. Seitz appears in the Appendix on page 36.

downloaded it. I utilized computer software to add the information that I wanted, and after I obtained a blank W–2 form from the IRS Web site, I took the completed documents with the fake identity information to the New Jersey Department of Motor Vehicles and obtained in short order a genuine New Jersey photo identification card. I feel that if I wanted to take the time and the effort, I could have easily used the same documents to obtain a genuine New Jersey driver's license.

During the time that I was searching the Internet for fake identification Web sites, 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.

I also made a fake driver's license by altering mine, using various computer programs, including Adobe Photoshop. After I had these documents, I went on the Internet and obtained car loans using the identity of people I found on the Web. When these loans were approved and I received checks, I went to the car dealers to attempt to purchase new vehicles with the false identification. For the most part, it was very easy. The new car dealers want to sell cars and pay very little attention to the details of identification.

I got cold feet the first time and I left, but the second time, the car dealer just accepted the fake ID, took the insurance binder I had previously secured, and a short time later, I was driving one of the most expensive vehicles off the lot. I eventually was discovered after the car dealer submitted the paperwork to DMV and they determined that the numbers of the fake driver's license were not valid. I realize what I did was illegal, but I also must say it was not very difficult to accomplish.

In conclusion, I found that there was a readily available supply of fake identification providers on the Internet. Anyone with some computer skills can download these templates for fake identification and produce some very high-quality documents. I feel that if Web sites, especially the U.S. Government Web sites, were prohibited from providing specific personal identifiers on the Web, such as Social Security numbers, that would make activities such as mine a lot more difficult. That is all.

Senator COLLINS. Thank you, Mr. Seitz. I would like to begin with you and ask you some questions about the phony documents that you created and used. I would like to have Exhibit 12 displayed.[1] It is my understanding you are familiar with these exhibits.

Mr. SEITZ. Yes.

Senator COLLINS. This exhibit contains the three documents that you used to commit your crimes. The name and address and Social Security number of a Richard Clasen is on two of these documents. Who is he and how did you happen to choose his identity?

Mr. SEITZ. Richard Clasen is a—he is a ranking executive with a company called EFI Electronics. I discovered his information and Social Security number, name, place of employment, and home information, it was his address and his phone number, from the Securities and Exchange Web site. Quarterly reports must be filed

[1] See Exhibit 12 which appears in the Appendix on page 89.

with the SEC, and that information is public. They publish that right on their Web site and he was just a random person off of there.

Senator COLLINS. So he was not someone whom you knew personally?

Mr. SEITZ. Oh, no.

Senator COLLINS. And all you had to do was go to a Web site that actually was maintained by the Federal Government and you were able to obtain this individual's—not only his name and his address, which one might expect—but his Social Security number and his telephone numbers, is that correct?

Mr. SEITZ. Correct.

Senator COLLINS. Have you used any other Web sites maintained by the Federal Government as a source of these kind of identifiers, the personal information?

Mr. SEITZ. Well, I also found that Congressional Web site—I am not too sure of the exact address—they put up—they publish the military nominations for promotions. I know they list the Social Security numbers, as well, of dozens, if not hundreds, of individuals.

Senator COLLINS. What we found in our investigation, after finding out about what you had been able to do with government Web sites, is that the *Congressional Record* no longer includes the full Social Security number of those military officers who are up for promotion. But the back editions, which are still available on some Web sites, do still contain that kind of information.

Mr. SEITZ. Correct. As of the last time I checked, you were just using the last four digits. But the previous *Congressional Records* still contained the full numbers.

Senator COLLINS. So this suggests to me that in addition to our need to look at strengthening the laws and going after more aggressively those who run these private Web sites, that we need to review the Web sites maintained by Federal agencies to make sure that they are not a source of information that could be used easily to commit identity fraud.

Mr. SEITZ. Correct.

Senator COLLINS. The third document I want to draw your attention to is the green document on the bottom of the exhibit. Now, is this the counterfeit birth certificate that you created from the template that you obtained from the Internet?

Mr. SEITZ. Yes, it is.

Senator COLLINS. The document says on it, "Do not accept this certificate unless the seal of the city is affixed hereon." Did you have any trouble getting or making the seal?

Mr. SEITZ. No. The reason I chose the City of New Brunswick as the one to download and use as a template is because it mirrors my birth certificate. I was born in the City of New Brunswick and it was something I had to compare, so it was fairly easy to create a plausible, or a fictitious document.

Senator COLLINS. And the seal was already on the downloaded document, is that correct?

Mr. SEITZ. Yes.

Senator COLLINS. Is the white document in the middle of the page the W–2 form that you also downloaded from the IRS Web site?

Mr. SEITZ. Correct. The IRS provides blank tax forms for almost all the forms that they have. It was just a matter of downloading it, inserting it in the printer, and finding the correct font in which to print on, and it came out, as you can see, it comes out pretty plausible.

Senator COLLINS. Why did you choose this document? What was your intent? What were you going to do with the W–2?

Mr. SEITZ. Well, as you said earlier, the 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.

Senator COLLINS. So what you did is you took the W–2 form which you had downloaded from the Internet and filled out, the phony birth certificate, which you also got from the Internet and filled out, and then took that to the Department of Motor Vehicles in New Jersey and got an actual driver's license, but with wrong data on it, correct?

Mr. SEITZ. Correct.

Senator COLLINS. Did anyone question either of the documents that you brought to DMV?

Mr. SEITZ. Not at all.

Senator COLLINS. I understand that you searched several Web sites during your search for false identification documents. Was this a lengthy process? Did it take you a long time to find the kinds of computer templates that were suitable for your purposes?

Mr. SEITZ. No. As Mr. Blalack earlier said, it is very simple. It is a matter of putting "fake identification" into a search engine and clicking on links that it returns to you. It takes a matter of minutes to find the sites.

Senator COLLINS. And was it difficult once you downloaded the template to actually make the hard copy, the physical copy of the documents?

Mr. SEITZ. No, it was not. It was very simple. Once I had obtained the—I guess the correct paper or the correct media to print it on—it was a matter of minutes.

Senator COLLINS. If you had not been able to do this as easily, would you have tried to find another source of false IDs outside of the Internet?

Mr. SEITZ. Probably not. I am very familiar with computers and it was just something that I came across. To tell you the truth, I have never—I do not know any other places to go get fake identification as good as on the Internet.

Senator COLLINS. As I was listening to you, that is exactly the point that occurred to me. It is probable you would not even know where to get a set of false identification documents. But because of your expertise with the computer and because of the ease with which you were able to locate these sites, download the information that you need, and then produce the documents, it was probably much more tempting to do so and much easier to do so.

Mr. SEITZ. Correct. It was familiar.

Senator COLLINS. In addition to the ease with which you could get these documents, were there other reasons why you chose the Internet as the source?

Mr. SEITZ. For its anonymity. As you said before, I can surf the Internet from my home, and from the library. No one knows who I am.

Senator COLLINS. Were you afraid that you might be detected as you searched?

Mr. SEITZ. No, because as I stated in my opening statement, I used a library, a public library. 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.

Senator COLLINS. And arguably, using the library's computer was much safer than using your own computer in your home as far as the ability of law enforcement to trace you.

Mr. SEITZ. Correct.

Senator COLLINS. In your written testimony, you said that you frequently encountered disclaimers, and you mentioned this in your oral statement, as well, as you searched the Internet for false identification documents. Did you notice if a disclaimer was posted on the Web site from which you obtained the false birth certificate?

Mr. SEITZ. I cannot remember if there was one on that specific site. I do remember encountering them on several sites, but on the one with the birth certificate, no.

Senator COLLINS. Did you think that the Web site operators were truly trying to discourage illegal use of their documents as you searched these sites?

Mr. SEITZ. No, I do not. 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 the disclaimer, they are probably, in my opinion, trying to cover themselves. It does not discourage anyone.

Senator COLLINS. Thank you, Mr. Seitz.

Agent Myers, you mentioned in your written statement that you have seen a significant growth in the use of high-quality identification documents and you believe that is because they are available on the Internet. In your statement, you had some statistics on the percentage that you thought of false IDs were attributable to the Internet and also the growth. Could you give us that information, to give the Subcommittee an estimate of the percentage of false IDs that you see that you believe the Internet is the source for?

Mr. MYERS. Yes. In my position as the State ID Fraud Coordinator with the Division, I receive thousands and thousands of IDs every year, usually in bags of 100 to 200 almost every week from either agents in the field, other law enforcement agencies, even some banks have sent me some false identification. It is my job to go ahead and look at the identification, gather the intelligence to find out, is it false and counterfeit, and what security features they have been able to reproduce in this type of false identification.

We have found within the past few months such high-quality counterfeit identification that it is virtually undetectable. I have specialized electronic equipment that I use and we have developed

in order to determine counterfeit from original when we cannot see it with our own human eye. Things like holograms, bar coding, micro printing, all of these are found on the new counterfeit identification cards.

We found approximately 2 years ago during an operation that we do every year on false identification approximately 1 percent, or a little less than 1 percent, came off the Internet. Last year, we found that a little less than 5 percent of the counterfeits came off the Internet. This year, we have determined there was approximately 30 percent of the counterfeit and false identification that we seized came from the Internet.

Senator COLLINS. So in just a 2-year period, the percentage of false IDs that you have seen for which the Internet is the source has gone from 1 percent to about 30 percent?

Mr. MYERS. Yes, Senator Collins. Also, we believe that by next year, we are going to find at least 60 to 70 percent of the IDs that we are going to be seizing coming from the Internet.

Senator COLLINS. So this is clearly an exploding problem and the Internet is becoming a very troublesome source of very high-quality IDs.

Mr. MYERS. Yes.

Senator COLLINS. And in general, are the IDs that have been produced using templates from the Internet higher quality than the IDs that you used to see because of the ability to incorporate the kinds of security features that you have mentioned?

Mr. MYERS. Much better. The graphics that can be produced on the computer, they can be electronically transmitted to anyone in the world in that same quality. Normally, what people would use would be a poorer quality of printing and colored paper and lamination procedures. Now, with the technology that is available, they can actually laser scan the entire document, including its hologram, and make it appear to be a true hologram and just electronically send it to anyone who purchases the access.

Senator COLLINS. Many States, such as Connecticut, have added the kinds of security features that you talked about in your presentation, and in the case of Connecticut, 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. Is that the problem you are seeing, that it is impossible for States to modify and add enough security features to keep pace with the ability of scam artists to duplicate exactly the same kind of security feature?

Mr. MYERS. Well, the problem we have, 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 these all types of legal identification.

Some of the features on the license that you showed, 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. Things like bar codes and even

2-dimensional bar codes that some States are going to are easily generated off the Internet. There are several sites that assist you in generating these security features.

Senator COLLINS. And even the magnetic stripe on the back has been able to be duplicated so that if this license were put through a machine, it would actually show a true driver's license, is that correct, too, in some cases?

Mr. MYERS. That is correct. It is very rare for us to find an electronically encoded mag stripe, but we have found a small portion of those.

Senator COLLINS. Given the growth of phony IDs over the Internet and the difficulty that most law enforcement officials would have in discerning that this is not a real ID, what is the answer? Do law enforcement officials have the proper training and the tools that they need? Are laws tough enough?

Mr. MYERS. Our agency focuses on the training issue. We find that very, very few law enforcement agencies train their people on the detection of false identification. Even I, as a former State trooper, received very, very little training on our own Florida driver's license.

We have been focusing on very detailed 4- and 8-hour classes for law enforcement people to determine certain counterfeit characteristics where they can make that determination. The issue of false identification is becoming very, very popular and with the growth of intelligence and information we are gathering, our training programs have to be updated virtually every month to come up with new technologies that are being used.

Senator COLLINS. One of the problems that the Subcommittee investigated is that law enforcement officials tend to focus on combating the crime that is committed with the false ID rather than focusing on shutting down Web sites that are selling illegal, bogus identification. Later today, we will hear the director of the Secret Service point out, as he has in his written testimony, that some form of false ID is a prerequisite for many financial crimes.

Since this is so, does not this fact suggest that a crackdown by law enforcement on the Internet sites that we have highlighted would, in turn, prevent other crimes from occurring, such as bank fraud and identity theft, if we went to the source of these documents?

Mr. MYERS. For every manufacturer of counterfeit identification that we raid and make arrests on, we feel that we are preventing tens of thousands of counterfeit IDs from hitting the streets. Some of it may be an alcohol issue. A lot of it is bank issues, identity theft, and many, many other crimes. We depend on identification for virtually every type of transaction that we deal with in today's society.

Our main focus is to look at these counterfeiting locations, because as you said, to find the crime, then locate the identification, is basically a long, drawn-out process when it would be much easier to locate those that are manufacturing the identification, especially on the Internet. Probably the biggest impact that we have seen on the Internet, as I monitor it and have for many years is the work that was done by your own Subcommittee's investigators. They had a dramatic impact on those on the Internet. Not even

knowing your investigation was going on, I could see that the activity on the Internet as it related to false ID was going through some changes.

Senator COLLINS. We have noticed that a lot of the Web sites that we identified early on are no longer in existence, but my fear is that once we complete our work in this area, that unless law enforcement starts being more aggressive in shutting down these Web sites, that they will just pop back up again.

Mr. MYERS. That is correct. We anticipate that any of those that were not arrested, and most were not due to certain problems with statutes, these people will be right back, and we have found in many cases that we have even arrested people for it, then we find them back on the Internet.

Senator COLLINS. Just a couple more questions for you. One is that we found that there are, in addition to false IDs, there are also documents that are phony that imply a person has completed a course or has been trained, for example, as a nurse's aide. That troubles me because that implies that another potential problem that we may have is the use of these phony credentials by people to get jobs for which they are not qualified and potentially that is a threat to public health and safety.

Similarly, the presence on the Internet of credentials for law enforcement officials I find frightening. The idea that someone could duplicate a police officer's ID or an FBI credential to gain access to someone to harm them, which may have happened in a case in the South that we are proceeding with, also adds a new and very ominous dimension.

I know we have talked a lot this morning about bank fraud and identity theft, but would you agree that other very serious crimes are a potential threat due to these credentials and law enforcement IDs being available via the Internet?

Mr. MYERS. That is very true, and what we have found, there are several Web sites, some of them harder to find than others, that will sell university degrees from universities and colleges around the United States. When law enforcement does a background check to hire someone, we do not just accept that diploma or degree. We require transcripts. And as we looked on the Internet, we found several of these sites also sold transcripts to go along with these documents, making it very, very difficult to determine the difference between true and false information. Sometimes they will use someone's name that actually graduated from these colleges, which a phone call check would confirm that the person did go there and did lawfully graduate.

The issue with law enforcement identification and credentials is a major issue. It has not been looked at very well. Most law enforcement credentials are much easier to copy and to counterfeit than driver's licenses. Most driver's licenses in most States have multiple security features. Most law enforcement identification is merely a picture stuck on a card and laminated.

Senator COLLINS. That is a very good point. Ironically, these driver's licenses have far more security features in them than the credentials for law enforcement officials that we found on the Internet, which were, as you point out, generally just a picture on a piece of paper with some information. They were extremely easy to

duplicate compared to the driver's licenses with more security features.

One final question for you. As a general rule, have you found any validity to the claim that these Internet site operators make that they are selling these phony identification documents or credentials solely for novelty or entertainment or educational purposes?

Mr. MYERS. That issue has come up quite a bit. There are certain Federal laws, like the "Not a Government Document" disclaimer. The laws in the State of Florida are very specific, which allows us to bypass those particular issues. If they issue a identification document with just a date of birth, they are required to meet certain guidelines.

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.

Senator COLLINS. The Subcommittee investigators also found that the novelty claim, even when printed on a license, was not indelible as the law requires and, in fact, was easily erased with a pencil eraser in many cases, or in the example I gave previously, the phony ID is enclosed in a laminated pouch from which the license can easily be used and, thus, no more disclaimer.

Mr. MYERS. That is correct.

Senator COLLINS. Thank you very much, Mr. Myers.

Mr. Blalack, just one final question for you. The Subcommittee, in the course of its investigation, made purchases from several of these Internet Web site operators. In a few cases, the Subcommittee's check was cashed but no product was provided, is that correct?

Mr. BLALACK. That is correct, Chairman Collins.

Senator COLLINS. This strikes me as the ultimate scam because someone who is purchasing a phony ID and gets ripped off by the Web site operator is very unlikely to file a complaint with the police.

Mr. BLALACK. That is exactly right, and in fact, Chairman Collins, one of these individuals we actually were able to make contact with and admitted that they had not sent the product and had advertised for the Web site intending not to provide the product because they had been ripped off themselves and were just trying to get their money back, so I think that is very accurate.

Senator COLLINS. I would note the Subcommittee is turning over those cases to the proper law enforcement authorities, but I bet we are the only one who has been ripped off by those Web sites who will file a complaint with the police.

Thank you very much to all of you. Your testimony was very helpful.

I would now like to welcome our final witness of the morning, Brian Stafford, the director of the U.S. Secret Service. Mr. Stafford was appointed director in 1999 after 29 distinguished years with the Secret Service, including many years as a field agent. Mr. Staf-

ford will testify regarding the proliferation of Internet crime and how the Internet facilitates identity theft and other serious crimes through the increasingly common use of false identification documents acquired online.

Mr. Stafford, I would like to welcome you this morning. We look forward to hearing your testimony. Pursuant to Rule 6, all witnesses are required to be sworn in, so I would ask that you stand and raise your right hand.

Do you swear that the testimony that you are about to give to the Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. STAFFORD. I do.

Senator COLLINS. Thank you. Please proceed.

TESTIMONY OF BRIAN L. STAFFORD,[1] DIRECTOR, U.S. SECRET SERVICE, WASHINGTON, DC

Mr. STAFFORD. Thank you, Madam Chairman. It is a pleasure for me to be here and for you to afford the Secret Service the opportunity to testify before this Subcommittee concerning the subject of false identification documents on the Internet and the Secret Service's efforts to combat this crime. I would like to thank the Chairman for your leadership in this area. The marketing of false identification documents on the Internet is a growing problem that requires the attention of law enforcement at all levels.

As a law enforcement bureau within the Department of Treasury, the Secret Service was created in 1865 to investigate and suppress counterfeit monetary instruments that affect the integrity and well-being of the Nation's financial infrastructure. In this role, the Secret Service has seen an expansion of its investigative authority commensurate with the evolution of payment systems, from paper to plastic and, most recently, to e-commerce.

The theft of personal information and other related data, often available through electronic media, has led to a significant increase in the production of false identification and the assumption of people's financial identity in the proliferation of financial crimes. Additionally, the Secret Service has witnessed the Internet become a tool for organized criminal groups to conduct these financial frauds through the production of false identification, the compromise of personal account information, and the ability to commit these crimes in a relatively anonymous environment.

Today, some form of false identification is a prerequisite for nearly all financial crimes. False identification provides criminals with the anonymity needed to conduct a myriad of fraud schemes.

To respond proactively to this growing problem, the Secret Service created a counterfeit instrument database. This database enables us to link cases of common origin through the forensic and investigative analysis of counterfeit financial instruments and identification documents. We are also enhancing our partnerships with both the law enforcement and financial communities through the use of our counterfeit check database. This database is available to the financial community as well as local, State, and Federal law

[1] The prepared statement of Mr. Stafford appears in the Appendix on page 38.

enforcement officers, thereby expediting the exchange of investigative information.

As the Internet continues to evolve, the ability for the criminal element to obtain false identification and compromise our financial systems from afar makes it imperative for law enforcement to combine personal resources and investigative expertise through the formulation of financial crimes task forces in cities on a national and international level. Task forces are not a new concept. In fact, the Secret Service started its first 11 financial crimes task forces in 1983. These initial 11 task forces are still in effect and we have expanded with 17 additional task forces, focusing primarily on financial crimes and organized criminal groups who are making use of the Internet.

The Internet has also led to information collection as a common byproduct of the newly emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by entrepreneurs intent on increasing their market share. It is estimated that there are currently more than 1,000 data warehouses. The ability to obtain online personal information coupled with the sale of false identification has allowed financial crimes to flourish on the electronic highway.

We have investigated numerous cases where criminals have used other people's identities to purchase everything from computers to homes. Financial institutions must remain vigilant, or they will fall victim to the criminal who attempts to obtain a loan or cash a counterfeit check using false identification.

The United States financial community makes $3.5 billion in electronic payment transactions per year utilizing various telecommunications systems. The financial community, private citizens, and private industry have migrated to the use of the Internet to conduct electronic commerce. The United States is moving to an electronic commerce society with a vastly decreased reliance on paper currencies. This migration to e-commerce has revolutionized the way business is conducted and is the forerunner to the truly global economy.

The Secret Service has responded to this type of fraudulent activity in several ways. In 1988, the Secret Service created the Electronic Crimes Special Agent Program. This is a group of highly trained special agents assigned to our field offices throughout the United States and abroad are tasked with the examination and collection of electronic evidence. These agents are routinely utilized in assisting Federal, State, and local law enforcement in combating a host of computer and Internet-related fraudulent activities.

This program is unique within the law enforcement community in that it utilizes only special agents who are trained and conversant with the elements of the violations under investigation. It permits the agents to be part of the search-and-arrest teams, allowing them immediate examination of the computer evidence and often leading to additional pertinent investigative leads. All examinations are conducted and documented within 10 days. And lastly, these agents provide a proactive and immediate response rather than seizing evidence and awaiting laboratory results.

In addition, the Secret Service continues to work with the G7 and G8 high-tech subgroup to address jurisdictional concerns and international obstacles in an effort to effectively deal with international criminal organizations.

Some very positive steps are being taken to address the misuse of false identification documents and to combat identity theft. The Secret Service will always encourage both business and law enforcement to work together to develop an environment in which personal information is securely guarded. The emotional toll on the lives of those whose identities have been compromised cannot be fully accounted for in dollars and cents. Everyone is responsible for protecting personal information.

We do not believe in nor are we in the business of inhibiting the free flow of information so vital to a free society. We do, however, believe that those identified as misusing personal identification for criminal purposes should be subject to punishment commensurate with the crime.

Madam Chairman and Members of the Subcommittee, I would like to personally thank you for raising the awareness of the current problem of the Internet as a vast and growing marketplace for false identification fraud and identity fraud. I will be keeping you up to date on the Federal response to this emerging problem. On behalf of the men and women of the Secret Service, I would like to thank you for your continued support of the Secret Service and law enforcement.

This concludes my prepared statements and I would be happy to answer any questions you may have.

Senator COLLINS. Thank you very much, Mr. Stafford.

During the course of the Subcommittee's investigation, we talked with law enforcement officials all over the United States who confirmed what we heard from Agent Myers this morning, that the manufacture of very high-quality IDs is a growing problem and most of these investigators were able to link it to the availability of the high-quality templates on the Internet. Has your experience been similar? Are you seeing bogus IDs that are much more sophisticated than ever before and are you able to link that increase and the sophisticated nature of the IDs to the Internet?

Mr. STAFFORD. Yes, I agree with everything you said. In almost every arrest we make in the area of financial crimes, whether it be bank fraud, credit card fraud, telecommunications fraud, computer fraud, there is usually a component of false identification. Most of the false identifications either come from, as you mentioned, 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.

Senator COLLINS. Then if we were able to crack down on Web sites that were providing these false identification templates or documents, is it not likely that we would see a corresponding decrease in financial crimes?

Mr. STAFFORD. That would be likely if it was possible to crack down on these numbers, but I would question whether we can do that. As I know you are aware, there are over 14 million Web sites

right now on the Internet and they are adding approximately 10,000 a day. For any entity, including the Secret Service, and I have a lot of confidence in our people, but for any one to be able to monitor that, would be extremely difficult.

Senator COLLINS. Well, the SEC, the Securities and Exchange Commission, has volunteers, a cadre of volunteers that surf the Net looking for securities scams. We have held hearings on securities scams on the Internet previously and the SEC obviously did not have the staff and the resources to have an ongoing effort with its own staff, but it put together a group of volunteers who regularly surf the Internet to identify those kinds of questionable sites.

Does the Secret Service do any kind of monitoring of the Internet to look for sites that are selling and marketing false identification documents?

Mr. STAFFORD. No, we do not. 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.

We do have a very good relationship with the Internet service providers and we have been very successful when certain Web sites come to our attention in negotiating and talking to the Internet service providers, and they usually will shut them down voluntarily.

Senator COLLINS. I would certainly agree that bank fraud and identity theft are far more serious crimes than the manufacture of false IDs, but, in fact, it is the manufacture of the phony IDs that allows the bank fraud or the identity theft to occur. 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 if we could somehow crack down on the manufacture and marketing of those IDs, some of the subsequent crimes would never be committed.

Mr. Seitz said today, for example, that if it had not been so easy for him to manufacture false IDs on the Internet, he never would have known even another source to get a false ID and, thus, he never would have committed the bank fraud with which he is now charged and in jail.

Mr. STAFFORD. Well, I agree with everything you are saying, Madam Chairman. It is a good idea to have volunteers search the Net and have hearings like this which make people aware of this huge issue. If we could eliminate some of these sites, it would drastically help with some of the other high impact, high-dollar financial crimes investigations.

The problem is, there are so many sites that policing may not be the answer. I am not sure standardizing or enhancing some of the security features and identification would help to solve the problem. I think probably the answer is research and development, maybe biometrics, and go in that direction versus trying to police all these false identification problems.

There are prosecution problems with these low dollar amount cases. It is very difficult, particularly on the Federal level, to come up with thresholds that would meet prosecutable guidelines and sentencing guidelines. We met with the Federal Sentencing Commission a few weeks ago and are asking them to enhance and strengthen some of the sentencing guidelines.

Senator COLLINS. Do we need tougher laws? Do we need to increase the penalties for these kinds of crimes?

Mr. STAFFORD. The statutes as they exist are pretty good right now. As you are aware, and I would like to thank you, in 1998, the Identity Theft Act was passed and you voted for that. It did put some strength in that law of identity theft by not just making it illegal to possess or produce but actually to assume somebody's identity. So right now, the statutes are fine. I would rather zero in on some of the—what happens afterwards, and as I mentioned, we are working on that aggressively as far as strengthening the sentencing guidelines.

Senator COLLINS. There is no doubt that the identity theft law passed in 1998 is a very helpful tool, but a lot of the law that pertains to false IDs was passed in, I think, 1982, and there are legal experts who have told us that there is some question about whether they need to be modernized to make it clear that it applies to documents downloaded from a computer, that the use of the word "document" in the 1982 law could be interpreted as not applying to a computer template, for example. I would like to ask you to work with the Subcommittee to review the basic laws applying to false IDs to see if they do need to be updated and strengthened.

Mr. STAFFORD. We will and we do need to continue to address those issues. As technology evolves, oftentimes legislation is required, as it was in 1998.

Senator COLLINS. I applaud the work that you are doing with the sentencing guidelines so that judges understand that this is a serious crime, but I do think we also need to work to deter the crimes from occurring in the first place by having tougher penalties, by having some high-profile prosecutions of people that might well deter others from setting up these Web sites.

I would like to show you one that is particularly blatant. During the course of the Subcommittee's investigation, we discovered a Web site, and I have had it blown up on the posterboard, called PromasterCards, and it offers phony identification documents.[1] This is a page from PromasterCard's Web site which openly boasts that it is breaking the law. As you can see, it says, "We are openly admitting that we are breaking State, Federal, and several European laws by providing IDs that are exact replicas in every detail of the current IDs provided from the countries on our list."

Now, we obviously were very interested in talking to the operators of PromasterCards, but we were never able to do so because they are located beyond our borders and, thus, not subject to our legal process. But, in fact, you can see that this Web site boasts that it moved from the United States because of troubles with law enforcement. It states, "We have now moved our Web site to the United Kingdom but continue to process orders from our clients

[1] See Exhibit 13 which appears in the Appendix on page 90.

from around the world from our studios in the New York area. In the next few months, we expect to be shut down again, but we will bound back as always from another part of the Net."

How do we combat this problem, given the ability of a Web site to operate from another country, or to pretend that it is operating from another country, or to shut down and open up the next day under a different identity? Is this part of the challenge that you face?

Mr. STAFFORD. Yes, it is a huge challenge and particularly when they shut down before we can get to them and then open up someplace else with a different name and a different identity. It creates even more of a challenge when they migrate overseas. As you know, we do not have, and we may be asking for, legislation for extraterritorial legislation for white collar crime. We have it for counterfeiting right now, but we do not have it for this. It would be very difficult unless there was a mutual assistance treaty. Also, you need similar laws and criminals must break the law in the country in which they reside also in order to extradite them back.

So I think for those criminals that are migrating overseas, answer is to seek additional legislation, specifically extraterritorial legislation where, if we could find them, we could bring them back and prosecute them.

Senator COLLINS. Is there any sort of international law enforcement effort underway now to deal with this problem?

Mr. STAFFORD. Yes, in the Secret Service alone, we have task forces in England, Germany, Lagos, and Nigeria. We have permanent personnel in 16 other countries.

Senator COLLINS. My final question to you deals with Mr. Seitz's experience in which he used government Web sites as a source of the personal data that he then entered into the phony identification documents that he downloaded from the Web. Do you think the Federal Government needs to do a better job of making sure that Federal agencies are not putting personal identification information on the Web sites that are readily available to the public?

Mr. STAFFORD. Yes, I do.

Senator COLLINS. Is there any effort underway that you are aware of on that?

Mr. STAFFORD. Yes, there is.

Senator COLLINS. Could you tell me about it?

Mr. STAFFORD. There have been some very high-profile cases lately in the news about exactly what you are talking about. I believe that everybody involved, including those of us in the government, have become very aware of what can happen with a lot of that personal identification. The safeguards are very important. We all have to be responsible for safeguarding that information, including those of us in the Federal Government.

We conducted a national summit on identity theft about 2 weeks ago in the Department of Treasury. Also, on our Web site, there are a lot of recommendations, on what not only government can do but what we can do as individuals.

Senator COLLINS. Director Stafford, I very much appreciate your testimony this morning and your pledge to work with the Subcommittee so that together we can come up with an effective means

to at least stop the growth of this problem. Is there anything further that you would like to recommend to us?

Mr. STAFFORD. Nothing, other than I would just like to add that I believe having hearings like this are extremely beneficial. Your leadership in this area is extremely beneficial and I would just like to thank you again for the opportunity to be here and to speak on some of these issues.

Senator COLLINS. Thank you very much. I am glad I asked you if you had anything to add. Thank you for your testimony and your cooperation.

I would like to thank all of the witnesses who testified today. The testimony has been very helpful to the Subcommittee as we continue our efforts to combat this burgeoning problem. The wide availability of false identification and credentials on the Internet poses a serious new threat to the integrity of government operations that depend upon identification. For example, many government benefit programs require identification of beneficiaries to make proper payments under these programs. In addition, law enforcement, and an untold number of security operations rely on identification documents to grant persons access to government property, information, and secured areas.

The private sector is equally dependent on proper forms of identification for commercial activities. As the testimony we have heard this morning indicates, counterfeit identification is a common tool and, indeed, a prerequisite for many financial crimes.

If the government and private sector are to have confidence in the integrity of the identification documents on which they rely, we must somehow strive to stay ahead of the technology that allows these Web sites to flourish. I am very concerned about the ease with which these high-quality phony documents could be distributed. My staff, while extremely talented, is not comprised of computer experts, and yet with very little time and just buying materials readily available at an arts and crafts store, they were able to duplicate and manufacture an unending number of very convincing phony IDs.

After hearing the testimony today, I am more convinced than ever that we need a crack-down 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 Web sites.

During the course of this investigation, the Subcommittee received assistance from a number of officials, officers, and individuals. I would like to thank all of the agencies involved. I also want to thank the staff of the Republican Conference for their help today with all the technical aspects of our presentation.

And finally, I would like to thank the Subcommittee staff who worked very diligently on this investigation during the past 5 months, particularly Lee Blalack, Rena Johnson, Kirk Walder, Leo Wisniewski, Eileen Fisher, and Mary Robertson. Again, I want to thank my staff for its hard work.

The Subcommittee is now adjourned.

[Whereupon, at 11:11 a.m., the Subcommittee was adjourned.]

APPENDIX

DEPARTMENT OF BUSINESS & PROFESSIONAL REGULATION

Jeb Bush, *Governor* Cynthia A. Henderson, *Secretary*

STATEMENT
OF
SPECIAL AGENT DAVID C. MYERS
IDENTIFICATION FRAUD COORDINATOR

FLORIDA DIVISION
OF
ALCOHOLIC BEVERAGES AND TOBACCO
DEPARTMENT OF BUSINESS AND PROFESSIONAL
REGULATION

FRAUDULENT IDENTIFICATION UNIT

JOSEPH MARTELLI, DIRECTOR

DIVISION OF ALCOHOLIC BEVERAGES AND TOBACCO - FRAUDULENT IDENTIFICATION PROGRAM
THE BOLXHAM BUILDING G-13 1940 N. MONROE STREET TALLAHASSEE, FLORIDA 32399-1020
TELEPHONE (TALLAHASSEE) (850)921-2681 OR (JACKSONVILLE) (904) 727-3580

I am pleased to testify today on the availability of false identification over the Internet. As part of the Florida Division of Alcoholic Beverages and Tobacco "ABT," Department of Business and Professional Regulation, I coordinate the Fraudulent Identification Investigation Program. This program was created to stem what we viewed as a growing problem of identification fraud.

The program we have established has several objectives, including:

- ✧ investigation of Internet false ID sales;
- ✧ fraudulent identification detection training for law enforcement and other audiences;
- ✧ technical review of ID scanning equipment;
- ✧ gathering intelligence on counterfeit identification used by individuals for illegal purposes; and
- ✧ enforcement of laws relating to the manufacture, sale and possession of fraudulent identification.

I have been involved with investigations into identification fraud for the past 10 years, and have coordinated Florida's identification fraud initiative for the past two years. My background is in electronics, and I have a special interest in the use of computers and the Internet to create false identification.

During the time I have investigated identification fraud I have seen many new techniques and methods of manufacturing false identification. In the past two years, one of the most dramatic and significant developments in the field of identification fraud has been the use of the Internet. The Internet now presents the largest potential opportunity to produce, market, and sell high quality false identification.

Based on my years of law enforcement experience, I estimate that approximately 30% of the false identification cards I see come from the Internet. About a year ago, the Internet may have generated about 5% of the fake IDs, and more than two years ago the Internet was responsible for only 1% of the fake IDs. The growth in the use of the Internet, combined with the advances in computer technology and the decrease in the cost of equipment used to manufacture ID cards, have led to a dramatic increase in the quality of false identification, and in the quantity that is produced with the assistance of the Internet.

As is the case with many forms of new technology, it is younger individuals who both adopt and become adept at using the Internet and computer technology. While it is with growing ease that youth can obtain fraudulent forms of identification, retailers and law enforcement officials find it increasingly difficult to distinguish valid from counterfeit forms of ID. The Internet allows the creation and widespread distribution of counterfeit identification

that duplicate many of the features of legitimate identification. Special security measures like holograms, microprinting and bar codes are already in use by counterfeiters on the Internet.

Our efforts to curb the use of false identification have resulted in eleven arrests in Florida for the sale and manufacture of counterfeit IDs. We have assisted with investigations in other states, producing four out-of-state arrests. Because there is no other state with a concerted program to investigate identification fraud, I believe this has stopped only a small portion of the false identification business.

As I mentioned previously, the Internet is fast becoming a major factor in the production and distribution of false identification. My background in electronics has enabled me to identify, monitor and track a large number of individuals who have used the Internet as a part of their false identification operation. Through special software we have identified counterfeiters on the Internet who appeared to be operating from out of the country, when in fact, they were found to be within the United States and some within the State of Florida. Shutting down one Web site may prevent tens of thousands of IDs from being produced.

Our effort to curb the use of the Internet as an outlet for the sale of false identification has resulted in 33 Internet sites being removed from the Web. Taking enforcement action against these sites is difficult for state and local law enforcement agencies. Just the act of locating the Web site can be a major task. Many operate outside the United States. Assistance from Federal agencies is very difficult. Very few agents, even on the state and federal levels, have any training in the area of counterfeit identification.

Despite our arrests and other action to stop the manufacture and use of false identification, this problems continues to grow. Over the past four months our unit in Florida has made more than 300 arrests for possession of false identification. These counterfeit IDs were used for a variety of criminal activities, including bank fraud and identity theft. During the same four month time period, several businesses confiscated and turned over to ABT over 5,000 counterfeit IDs. These phony IDs consisted of everything from state driver's licenses, to military identification cards, to identity cards from numerous foreign countries. The fact that so many different forms of identification are used illustrates how difficult it is for most individuals to verify the authenticity of identification documents. Not only is it difficult for someone working at a bank, for example, to recognize the features that authenticate a driver's license from a distant state, but that bank official might also be presented with a number of types of foreign identification.

Even experienced law enforcement officers may have difficulty in detecting false identification. Many states use several security features on their driver's licenses, but in some instances the features are not even disclosed to law enforcement or other authorized individuals. One state, for example, used microprinting on its license, but that security feature was not known to other individuals in the office issuing the license.

In addition, many law enforcement individuals receive little training in detection of identification fraud. One of the efforts of my agency has been to assist in educating those who must examine identification. As a response to the growth in identification fraud, in the past twelve months my unit in Florida has conducted training for over 96 local, state and federal law enforcement agencies. This training has provided the over 1,200 officers in attendance with new intelligence and guidance in the development of ID fraud cases. Our outreach program also conducts educational programs for retailer groups to assist them in determining the validity of identification used for alcohol or tobacco purchases.

A large percentage of high quality counterfeit IDs I have reviewed were purchased via the Internet. Many counterfeiters who manufacture fake identification have advised my unit that the templates used to create the identification were received from the Internet. Computer technology not only makes it relatively simple to create the basic template allowing the counterfeit document to be produced, but allows the transfer of that template via e-mail and other Internet communication devices.

Based on our investigations, I believe Internet sales of false identification have increased dramatically. Current Web sites offer to sell identification for all 50 states. Those operating Web sites who offer to manufacture false identification often have sophisticated printing equipment which allows the production of high-quality counterfeit identification. These high-quality identification cards can be purchased by anyone, in any name, with any date of birth, for prices ranging from $30 to over $300. Internet savvy individuals, often those in college, but even many high school or middle school students, are able to quickly find a vast array of information on false identification. My conversations with several teachers in Florida schools indicate that a large number of students know just how to use the Internet to obtain false identification.

Several statistics demonstrate the popularity of Internet sites selling false identification materials. Some false ID sites have received over 10,000 inquiries on a single day. Based on our investigations, the annual income of Internet ID sales can exceed $1,000,000 per year by a single operator.

Individuals using templates to create their own fake identification have taken advantage of the current technology and the lower prices for high-quality computers and printers to manufacture their own fake IDs, some of which are very high quality. These personally made fake IDs may use digital photographs and replicate holograms used by various states. Again, the Internet provides assistance not only through availability of many different templates, but through Web sites that offer instructions on the materials and methods needed to make a hologram or laminate a counterfeit ID.

Let me briefly describe two instances of individuals who have used the Internet to sell false identification. Fortunately, law enforcement has been able to shut down both of these

operations, but when they were in operation, they were able to produce a large number of high-quality identification cards.

The first Web site, operated by Josh Dansereau, made several high-quality false state driver's licenses. In an undercover capacity, I communicated with this individual by e-mail, and was able to track down his location using special computer software. Mr. Dansereau was later notified of the official investigation and he allowed me to search the house he used for his operation, where I found 85 envelopes containing fake IDs that were about to be mailed. Many IDs were to adults in their mid 30's and 40's in attempt to avoid law enforcement or commit fraud.

The second Web site, operated by Robert Sek, also marketed false identification through sales representatives on college campuses. Through a confidential informant, I obtained information about this operation, which was based in Austin, Texas. I turned my information over to the Texas Alcoholic Beverage Commission and the United States Secret Service, who subsequently executed a search warrant on the apartment where Mr. Sek operated. The IDs he made were high quality, and Mr. Sek told me that he made over $1,000,000 from his sales of fake IDs. With the money he had made, he had planned to expand his operation and retain his own private attorney.

These two individuals represent only a small fraction of the Internet operations selling false identification. The State of Florida plans to continue our aggressive efforts to combat false identification and to curb the use of the Internet to manufacture and sell false identification. I appreciate the efforts of this Subcommittee to highlight this important issue.

✧✧✧

Statement
of
THOMAS W. SEITZ
Hearing On
Phony IDs and Credentials Via The Internet – An Emerging Problem
May 19, 2000

My name is Thomas W. Seitz. I am originally a resident of the State of New Jersey and I am presently incarcerated at the Baker County Jail located in Macclenny, Florida. I am 23 years old and I am currently serving a prison sentence imposed by the State of New Jersey after I was convicted and sentenced to 3 years for committing the crimes of theft by deception, forgery and uttering a forged instrument. I have also pled guilty to bank fraud and I am awaiting sentencing by the United States District Court, Middle District of Florida.

I appreciate the opportunity to testify before this Subcommittee. I hope that I can show its members how relatively easy it is for someone to engage in obtaining information from the Internet, including such personal information as Social Security numbers. Moreover, I hope to show how easy it is to craft phony identification using that information and obtain significant amounts of money with little effort.

I consider myself to be fairly well versed in the use of computers. I have worked with computers since the 6th grade and was employed as a network engineer. I obtained via the Internet, names, social security numbers, and addresses of people by accessing files maintained as public record on the Securities and Exchange Commission Web site. Although at first I did not have the intent to defraud anyone, I started searching the Internet again and determined there were a large number of sites that offered the means to make fake identification and the opportunity presented itself.

I used a computer at the library in Old Bridge, New Jersey and accessed various Web sites that offered documents for downloading including birth certificates and driver's licenses. Some were free so I found one that offered a New Jersey birth certificate and downloaded it. I utilized computer software to add the information I wanted and after I obtained a blank W-2 from the IRS Web site, I took the completed documents with the fake identity information to the New Jersey department of Motor Vehicles and obtained in short order a genuine State of New Jersey photo identification card.

I feel that if I wanted to take the time and effort, I could have used the same documents and obtained a genuine driver's license as well. During the time I was searching the Internet for fake identification Web sites, I frequently came across disclaimers on the individual sites that would say "for novelty use only." I can't think of any reason why a statement like that would be there. It did not deter my actions in any way. I did make a fake driver's license by altering mine using various computer programs including Adobe Photoshop.

After I had the documents, I went on the Internet and obtained a car loan using the identity of people I found on the Web. When these car loans were approved and I received checks, I went to the car dealer to attempt to purchase new vehicles with false identification. For the most part, it was very easy. The new car dealers want to sell cars and pay very little attention to the details of identification. I got cold feet and left the first time I tried to buy a car with fake identification. The second time, the car dealer just accepted my photocopied fake driver's license, took the insurance binder I had previously secured and a short time later, I was driving one of the most expensive vehicles off the lot. I eventually was discovered after the car dealer submitted the paperwork for licensing and the DMV determined the numbers that I used for the driver's license were not valid. I realize what I did was illegal, but I would also say that it was not very difficult to accomplish.

In conclusion, I found that there was a readily available supply of fake identification providers on the Internet. Anyone with some computer skills can download the available templates for fake identification from the fake identification Web sites and produce some high quality fake documents. I feel that if Web sites, especially United States Government Web sites were prohibited from providing specific personal identifiers on the Web, such as Social Security numbers, it would make activities such as mine a bit more difficult.

#

Department of the Treasury
U.S. SECRET SERVICE

Statement of Brian L. Stafford

Director, U.S. Secret Service

For Presentation to the
Committee on Governmental Affairs
Permanent Subcommittee on Investigations

May 19, 2000

Madam Chairman and members of the Subcommittee, I am pleased to be here today, and to be afforded the opportunity to address this Subcommittee concerning the subject of false identification documents on the internet, and the Secret Service's efforts to combat this problem.

As a law enforcement bureau within the Department of the Treasury, the Secret Service was created in 1865 to investigate and suppress counterfeit monetary instruments that affect the integrity and well-being of the nation's financial infrastructure. In this role, the Service has seen an expansion of its investigative authority commensurate with the evolution of payment systems from paper to plastic and, most recently, E-Commerce. The theft of personal information and other related data, often available through electronic media, has led to a significant increase in the production of false identification and the assumption of people's financial identity in the proliferation of financial crimes.

We concur with the Subcommittee's assessment that the availability of false identification on the internet is a problem, and we believe it is a growing problem, to which we plan to devote additional resources and attention.

Based upon the Secret Service's historic expertise in counterfeit currency investigations, Congress saw fit to expand this jurisdiction to encompass all forms of counterfeit financial instruments, as well as identification documents. As we move into the electronic commerce environment, the Secret Service has seen the compromise of global payment systems through credit card and other access device fraud, fraudulent identification, bank fraud, telecommunications fraud, and financial fraud relating to computer intrusions, often with the use of false identification.

Recent trends in criminal activity have taught us that these crimes are regularly committed by inherently violent organized criminal enterprises. Since it would be difficult to fully explain our entire investigative program in the area of financial crimes in this short statement, I have chosen to concentrate on the methods in which identity theft and false identification are used to commit financial fraud.

Many of our financial institution fraud investigations, to include access device fraud, counterfeit commercial checks and traveler's check fraud, and other forms of internal financial institution fraud, are predicated upon identity theft and false identification. Additionally, the Service has witnessed the Internet become a tool for organized criminal groups to conduct financial frauds, through the production of false identification, the compromise of personal account information and the ability to commit these crimes in a relatively anonymous environment.

False Identification

Today, some form of false identification is a prerequisite for many financial crimes, whether it is an identity takeover or the production of counterfeit identification. False identification provides criminals with the anonymity needed to perpetrate a myriad of fraud schemes. Often, in their attempts to remain anonymous, criminals may randomly assume the identity of another individual through the creation or purchase of false identification documents. In these cases, the goal may not be to target an individual for purposes of stealing his or her identity. Yet, these individuals' identities have been compromised through the use of their personal information.

The Secret Service currently investigates a variety of fraud schemes that utilize false identification documents. In 1982, with the passing of the Comprehensive Crime Control Act, the Service was given jurisdiction in the investigation of false identification documents. Since that time, we have investigated numerous financial fraud crimes which rely upon the use of fraudulent identification documents such as:

- social security cards;
- state driver's licenses;
- birth certificates;
- passports/visas;
- voter registration cards; and
- alien registration cards.

The use of these documents to perpetrate fraud has evolved from simply a means of fraudulent identification into actually assuming an innocent person's identity. Through the use of sophisticated "desktop publishing" equipment, such as computers and color laser copiers, and the advent of false identification merchant sites on the Internet, criminals are able to easily create the appearance of genuine documents utilizing someone else's personal identifiers. False identification documents and altered, counterfeited, or fraudulently obtained genuine identification documents, are routinely used with loan and check fraud schemes, almost all credit card fraud schemes, as well as immigration and passport fraud schemes.

One popular scheme is to use false identification to cash counterfeit checks. These checks are cashed at financial institutions and small businesses to receive cash and merchandise. By the time these checks are identified as counterfeit, the criminals are long gone. This scheme has been recently updated through the use of Internet banking. The Internet allows the criminal element to open on-line bank accounts with false identification, often in the electronic form. Once the account has been opened with a nominal amount of money, the criminals, through the use of desktop publishing, deposit counterfeit corporate checks. These checks are scanned and are virtually identical to the genuine item. These counterfeit instruments will clear and the criminal will empty the accounts through debit cards they received when they opened the account. These debit cards now become a genuine piece of identification utilizing a false identity. The checks will not be identified as counterfeit until that business or corporation clears their checking account, by which time the criminals have long departed. Since a large portion of this crime is done on-line, there are very few investigative leads.

The Secret Service recently investigated a large counterfeit check operation that originated in southern California and involved an organized criminal group. This group was manufacturing counterfeit checks and counterfeit identification through the use of advanced reprographics and desktop publishing. Although the scope of this activity was first identified by the Secret Service approximately 3 years ago and numerous arrests and prosecutions have ensued, the activity continues today.

In addition, we have assisted the Immigration and Naturalization Service with numerous investigations of false identification plants manufacturing counterfeit social security and alien registration cards for use by illegal immigrants.

In an effort to be proactive to this growing problem, the Secret Service has created the Counterfeit Instrument Database. This database enables us to link cases of common origin through a forensic and investigative analysis of counterfeit financial instruments and identification documents. We are also enhancing our partnerships with both the law enforcement and financial communities through the use of our Counterfeit Check Database. This database is available to security personnel in the financial community as well as local, state, and federal law enforcement officers, thereby expediting the exchange of investigative information.

We believe in the partnership approach. As the Internet continues to evolve, the ability for the criminal element to obtain false identification and compromise our financial systems from afar makes it imperative for law enforcement to combine personnel resources and investigative expertise through the formulation of financial crimes task forces in cities on a national and international level. Task forces are not a new concept; in fact, the Secret Service started its first 11 financial crimes task forces in 1983 targeting Nigerian Organized Crime. The Nigerian Organized Crime groups have always been prolific in committing financial crimes through the compromise and production of false identification. With the explosion of the Internet, we have witnessed this organized criminal group utilize the Internet for the production of counterfeit financial instruments, documents and false identification. These initial 11 task forces are still in effect and we have expanded with 17 additional task forces focusing primarily on financial crimes and organized criminal groups.

Social Security Identity Fraud

Although various forms of identification can be used to compromise the identity of someone else and commit financial crimes, the social security number appears to be the most popular. The totality of identity fraud/theft involving social security numbers is currently unknown due to the criminal activity not being reported accurately. There are a variety of fraudulent purposes for which criminals misuse social security numbers because the number itself has become a form of identification. The Internet has allowed this form of identity theft to be committed in an electronic format.

Historically, the social security number was established as a means to coordinate payment and receipt of social security benefits, not as a form of identification. The Secret Service has seen social security numbers stolen and misused for numerous criminal purposes such as:

- to obtain employment;
- to disguise true identity from law enforcement; and
- to obtain credit and services.

The Information Age and Identity Fraud

As we enter the new millennium, the strength of the financial industry has never been greater. A strong economy, burgeoning use of the Internet and advanced technology, coupled with increased spending has led to fierce competition within the financial sector. Although this provides benefits to the consumer through readily available credit, and consumer-oriented financial services, it also creates a rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Information collection has also become a common by-product of the newly emerging E-Commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by entrepreneurs intent on increasing their market share. This has led to an entirely new business sector being created which promotes the buying and selling of personal information.

With the advent of the Internet, companies have been created for the sole purpose of data mining, data warehousing, and brokering of this information. These companies collect a wealth of information about consumers, including information as confidential as their medical histories.

Consumers routinely provide personal, financial, and health information to companies engaged in business on the Internet. Consumers may not realize that the information they provide in credit card applications, loan applications, or to merchants they patronize, are valuable commodities in this new age of information trading.

Data collection companies like all businesses are profit motivated and, as such, may be more concerned with generating potential customers rather than the misuse of this information by unscrupulous individuals. This readily available personal information, in conjunction with the customer friendly marketing environment, has presented ample opportunities for criminals intent on exploiting the situation for economic gain.

A 1999 Washington Post article mentioned that there are approximately 1,000 data warehouses, which is 10 times the amount that was in existence just 5 years ago. Information brokering is here to stay and will probably increase in the near future. The Washington Post also recognizes the fact that there are few laws restricting the collection of data, and federal agencies have been able to combat this problem only by advising industry to be diligent. The ability to obtain on-line personal information, coupled with the sale of false identification, has allowed financial crimes to flourish on the electronic highway.

We have investigated numerous cases where criminals have used other people' s identities to purchase everything from computers to houses. Financial institutions must continually practice due diligence lest they fall victim to the criminal who attempts to obtain a loan or cash a counterfeit check using someone else's identity.

As financial institutions and merchants become more cautious in their approach to "hand to hand" transactions, the criminals are looking for other venues to compromise. Today, criminals need look no further than the Internet.

A recently publicized Internet fraud investigation by the Secret Service, Department of Defense, Postal Inspection Service, and the Social Security Administration Inspector General's Office highlighted the ease with which criminals can obtain personal information through public sources. These defendants accessed a web site that published the promotion list of high-ranking military officers. This site further documented personal information on these officers that was used to fraudulently obtain credit, merchandise, and other services.

In this particular case the financial institution, in an effort to operate in a consumer friendly manner, issued credit over the Internet in less than a minute. Approval for credit was granted after conducting a credit check for the applicant who provided a "true name" and matching "true social security number." All other information provided, such as the date of birth, address, and telephone number that could have been used for further verification, was fraudulent.

The failure of this bank to conduct a more comprehensive verification process resulted in substantial losses and, more importantly, a long list of high-ranking military officers who became victims of identity fraud. This case exemplifies the theft and electronic use of the social security number as a form of identification.

The present-day United States financial community makes 3.5 billion electronic payment transactions per year, utilizing various telecommunication systems. The financial community, private citizens and private industry have migrated to the use of the Internet to conduct electronic commerce. The United States is moving to an electronic commerce society with a vastly decreased reliance on paper currencies. This migration to E-Commerce has revolutionized the way business is conducted and is the forerunner to a truly global economy.

Some projections indicate that by the year 2005, there could be one billion users on the Internet. This equates to one billion potential customers. The Internet is accessible to anyone with a computer, modem, and access through various service providers.

The ever-expanding use of the internet heightens our concern about the potential for greater criminal activity using false identification acquired from the internet.

Responses to the Problem

In response to this burgeoning high tech revolution, the Secret Service created the electronic crimes special agent program (ECSAP), a group of highly trained special agent personnel assigned to our field offices throughout the continental United States and abroad, tasked with examination and collection of electronic evidence. These agents are routinely utilized in assisting federal, state and local law enforcement, as well as computer industry personnel, in combating a host of computer and Internet related fraudulent activities.

This program is unique within the law enforcement community in that it utilizes those special agents who are trained and conversant with the elements of the violations under investigation.

The program permits agents to be part of the search and arrest teams, allowing an immediate examination of the computer evidence and often leading to additional pertinent investigative leads. All examinations are conducted and documented in a 10-day period. And lastly, these agents allow for a more proactive and immediate response, rather than a seizure of evidence and awaiting laboratory results.

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement departments that generally act as the first responders to their criminal activities. By working closely with other federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise which bridges jurisdictional boundaries.

In addition, the Secret Service continues to work with the Department of Justice and the G7/G8 high tech subgroup to address jurisdictional concerns and international obstacles in an effort to effectively deal with international criminal organizations. The Secret Service has learned that several foreign countries do not even have the statutes to prosecute defendants involved in electronic commerce fraud, such as data base intrusions, skimming of credit cards and credit card generating programs.

Personal and sensitive information about on-line subscribers and shoppers are, at times, innocently stored in unsecured databases which can be accessed through poorly protected web sites. Web site architecture and design often vary, allowing differing degrees of vulnerability.

Bank customers who find the idea of on-line banking appealing should be aware that the Internet is a public medium to conduct transactions and that the prospect of unauthorized access to personal information by Internet abusers is real. Certain controls that exist to address privacy concerns in the context of credit cards, credit agencies, and banks can and should be applied to electronic payments.

The Secret Service has found that, in general, the major Internet Service Providers (ISP's) are constantly updating security measures and have been receptive in establishing liaison with law enforcement in its goal to preserve the integrity of the Internet. However, we must realize that the Internet has vulnerabilities that can allow confidential business information and sensitive personal information to be compromised. Discussions are currently underway between the government and the ISP's to establish an association similar to other partnerships designed to share concerns and discuss issues among its members and law enforcement.

There are numerous security programs and features available to those who conduct business and communicate on the Internet to minimize Internet fraud and protect sensitive information. Many merchants and others who transact business on the Internet have successfully designed and implemented systems which reasonably ensure the integrity of sensitive information and transactions. These safeguards range from intrusion detection systems (IDS) to firewalls to chip technology associated with credit cards.

In addition, Internet service providers should not establish and instantaneously authorize an account or e-mail address for their customers based solely on a credit card number provided by that customer over the telephone or transmitted via computer. The ISP should authenticate the credit card and the user prior to allowing access. Merchants conducting business on the Internet should know their customers, and service providers should take steps to know their merchants.

Conclusion

As you have heard in this testimony some very positive steps are being taken to address the misuse of false identification documents and to combat identity theft. The Secret Service will always encourage both business and law enforcement to work together to develop an environment in which personal information is securely guarded. In this age of instant access, knowledge is power. We cannot allow today's criminals to abuse the very systems that were created for the betterment of society.

We do not believe in, nor are we in the business of, inhibiting the free flow of information so vital to a free society. We do, however, believe that those identified as misusing personal information for criminal purposes should be subject to punishment commensurate with the crime. The concepts of criminal prosecution for the perpetrators, restitution for the victims, and ethical responsibilities for those earning a living through the use of personal information are noble goals.

The Secret Service acknowledges that false identification and its availability on the internet is a very real problem, and we pledge our support in the Federal Government's efforts to eliminate it.

Madam Chairman and members of the Subcommittee, on behalf of the men and women of the U.S. Secret Service, I would like to take this opportunity to thank you for your leadership in this area, and your continued support of the Secret Service and law enforcement.

This concludes my prepared statement. I would be happy to answer any questions that you or any other member of the Subcommittee may have.

Thank you.

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 1

Certificate of Attendance

American State University

This certifies that
Susan M. Collin

Motor Vehicle Services — NEW JERSEY
C2963 26763 09772
CLASS D ENDR:
RESTR:
AUTO OPERATOR LICENSE
DOB 12-07-52 EXPIRES 03-31-2001
SUSAN COLLINS
123 YOUR STREET
JERSEY CITY NJ 07305
SEX F EYES BRO HT 5
X Susan
ES X197171
Ohio Health Ce
in cooperati
Association of Ohio Philanti
o Departm
apeutic Re
STATE
MAY 26,

Boston University
STUDENT IDENTIFICATION
Signature
SAN M.
CATION ONLY

The Sunshine State
LICENSE NUMBER
L252-784-51-465-0
SUSAN COLLINS
524 DRIVE ST.
ORLANDO, FL 32332
BIRTHDATE 12-13-76 SEX F HGT 5-6 REST A ENDORSE F
ISSUED 12-03-96 EXPIRES 12-24-02 DUPLICATE 12-07-96
DRIVER LICENSE CLASS D
Florida
ORGAN DONOR
Operation of a motor vehicle constitutes consent to any sobriety test required by law.

NON-TRANSFERABLE
PRESS
First SUSAN
Last COLLINS
Position PHOTO.
Event GALLERY OPENING
1003691112099

Kent State Univ
SAFE DRIVER

Certificate
Susan M. Collins
the
linators Program

OFFICIAL
PRESS
SUSAN M. COLLINS
U.S. SENATE
REG. NO. 01162

OHCA Certifying Officer

ARMED FORCES OF THE UNITED STATES
RANK/PAY GRADE SPC/E4
SIGNATURE
SUSAN M. COLLINS
GENEVA CONVENTIONS IDENTIFICATIO

DRIVER LICENSE MICHIGAN BUCKLE UP
MICHIGAN DRIVER LICENSE NUMBER C 963 26763 09772
ISSUED M153112
EXPIRES ON BIRTHDAY 01
NAME SUSAN COLLINS
ADDRESS 142 YOUR ST
CITY PERRY
DATE OF BIRTH 09 02 77
SEX F HEIGHT 5 6 RES CO
SIGNATURE X Susan

WYOMING
DRIVER LICENSE
129822-209
SUSAN COLLINS
145 OAKLAND WAY
LANDER, WYOMING 82520
CLASS: C ENDORS:
SEX: F HT: 5-06 WT: 120 DONOR:
HAIR: BRO EYES: BLU DOB: 1952/12/07
REST: SSN: 129-23-4543
Susan M. Collins
1997/08/05 106-0002
EXP: 2000/12/07

Connecticut
SUSAN
COLLINS
TALLMO

AUTHENTIC

FAKE

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 2

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 3

Fake ID is our only business!!

idSolution%.com

The leading source for all your identification needs...

NEW!!

New Identity Kit GO

A complete package that allows you REALLY become someone else

NEW!!

I.D. Templates on CD GO

A complete package that allows you to make your own I.D.'s from home...

FAST!

Electronic ordering

We now offer Electronic ordering on all of our product's. This allows us to complete your order and get it back to you in under 5 days.

alternative identification documents are our specialty. We provide you with the best quality documents you will find anywhere on the internet as well as the fastest service.

At http://www.idsolution.com. Youll discover an easy to use, information packed web site.

Fake id, fake birth certificates, fake passports are our only business. We utilize the latest equipment when manufacturing your id to ensure you the highest quality id available anywhere. We are simply the best at what we do and you need to look no further than here. We are your number one source for these documents on the web and will provide you with what you expect.

NEW!!

New Identity Kit GO

A complete package that allows you REALLY become someone else

idSolution%.com

The leading source for all your identification needs...

NEW IDENTITY KIT

This package allows you to obtain original identification from the Department of Motor Vehicles in the United States and Canada (please check with your local office to verify the documents you will be required to present).

We have taken the best document's we have and combined them under one complete package for a discounted price in excess of 50% if you were to buy the same items separately.

The package consists of the following:

1. American or Canadian Birth Certificate
2. FedEx employee photo identification card complete with FedEx holograms and magnetic swipe.
3. AT&T Long Distance bill complete with the name and address you supply us with
4. National propane bill complete with the name and address you supply us with
5. TCI cable bill complete with the name and address you supply us with

The majority of DMV departments will need a photo ID along with a certified birth certificate and proof of residence that is supplied in the form of Utility bills with your address on them.

We guarantee that the authenticity of these documents will be unmistakable from the original counterparts.

Please contact your local office before ordering. We will assist you in any way possible. If there is another document you must have contact us and we may be able to assist you .

PRICE $125.00 US

For ordering information please contact us identitykit@idsolution.com

1. American or Canadian Birth Certificate
2. FedEx employee photo identification card complete with FedEx holograms and magnetic swipe.
3. AT&T Long Distance bill complete with the name and address you supply us with
4. National propane bill complete with the name and address you supply us with
5. TCI cable bill complete with the name and address you supply us with

Senate Permanent Subcommittee
On Investigations
EXHIBIT # 4

MAINE DRIVERS LICENSE

ISSUED	EXPIRES	CLASS
00/00/00	00/00/00	C

LICENSE NO	BIRTHDATE
1234567	00/00/00

RESTRICTIONS	ENDORSEMENTS

HAIR	EYES	HEIGHT	WEIGHT	SEX
BR	BR	1'1"	100	M

SIGNATURE

JOE, SHMOE

PO BOX 1

SOMEPLACE, ME 12345

Secretary of State
Dan Gwadosky

2
3

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 5

MAINE DRIVERS LICENSE

ISSUED	EXPIRES	CLASS
09-21-96	09-20-02	A

LICENSE NO	BIRTHDATE
5423234	09-20-78

RESTRICTIONS	ENDORSEMENTS
AW	PX

HAIR	EYES	HEIGHT	WEIGHT	SEX
BR	BL	5 09	160	M

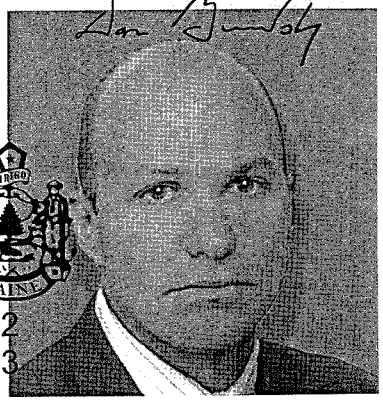
SIGNATURE

Lee Blalack

LEE BLALACK
321 MAIN STREET
AUGUSTA, ME. 04330

DIRIGO MAINE

Secretary of State
Dan Gwadosky



23

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 6

Fake ID Kit Ver 2.0 - Including official college transcripts you customize, college diplomas, new birth certificates, green cards, social security cards, updated drivers license, plus more! For more info on what comes with the kit, please follow the link below..

What Files Are Included? - For a complete list of every file that is included with the Fake ID Ver 2.0 kit, Click Here!

Samples - Here are some samples of our templates, if you would like us to add a sample template, please let us know.

- Social Security Card
- College Transcripts
- Green Card
- Birth Certificate
- College Diploma
- Drivers License

Instant Access! You can now get everything included with our kit, for a one time fee of $19.95 .

Welcome to the new and improved "*Fake ID Zone*" Here are some of the things that we offer on this site:

- **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.**
- **You will be given access to download 100+ templates that you can use to create your own fake ids. Our templates consist of birth certificates, green cards, college transcripts, college diplomas, drivers license, gun license, back stage passes, and much more. As of 10/1/1999 our collection of templates will be updated on a regular basis.**
- **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.**

We normally charge **$39.95** for our fake id kit on CD. If you order now you will receive a ***50% discount!*** *Receive instant access for* ***$19.95.***

Click Here To Order

Members Entrance

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!

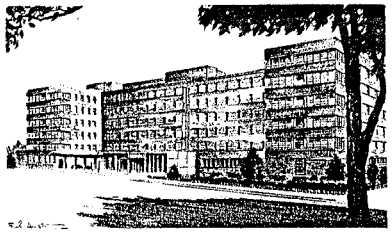
Senate Permanent Subcommittee
On Investigations

EXHIBIT # 7a.

AUTHENTIC

Victory Memorial Hospital

Waukegan, Illinois



This Certifies that _____

was born in the Victory Memorial Hospital of the City of Waukegan

on the _____ day of _____ A.D. 19__

In Witness Whereof the said Hospital has caused this Certificate to be signed by its duly authorized officer and its Corporate Seal to be hereunto affixed.

Timothy J Harrington

Administrator

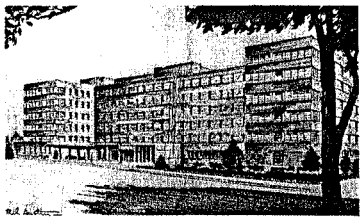
Attending Physician

Senate Permanent Subcommittee
On Investigations
EXHIBIT # 7b.

FAKE

Victory Memorial Hospital

Waukegan, Illinois



This Certifies that _____
was born in the Victory Memorial Hospital of the City of Waukegan
on the _____ day of _____ A.D. 19__

In Witness Whereof the said Hospital has caused this Certificate to be signed by its duly authorized officer and its Corporate Seal to be hereunto affixed

_____
Administrator

_____
Attending Physician

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 8a.

Kent State University

Certificate

Susan M. Collins

has successfully completed the

Nursing Home Resident Activity Coordinators Program

Presented by

the College of Special Programs

in cooperation with

the School of Home Economics
and the Gerontology Center

3.6 CEU

MAY 26, 1996

Instructor

Dean, College of Special Programs

G8061 541

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 8b.

Ohio Resident Activity Coordinator Training Project

Certificate of Attendance

IN RECOGNITION OF YOUR SATISFACTORY COMPLETION

OF THE SHORT TERM TRAINING COURSE FOR

ACTIVITIES PERSONNEL IN LONG TERM CARE FACILITIES

THIS CERTIFICATE OF ATTENDANCE IS AWARDED TO

SUSAN M. COLLINS

on behalf of the

American Health Care Association

Ohio Health Care Association

in cooperation with the

Association of Ohio Philanthropic Homes for the Aging

Ohio Department of Health

Ohio Therapeutic Recreation Association

at

KENT STATE UNIVERSITY

MAY 26, 1996

Date

Instructor/Coordinator

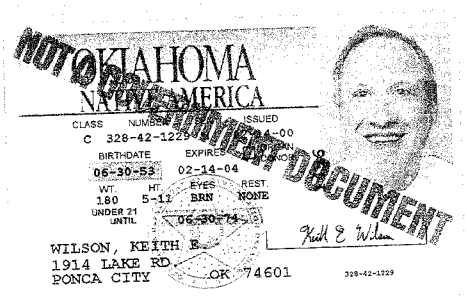
OHCA Certifying Officer

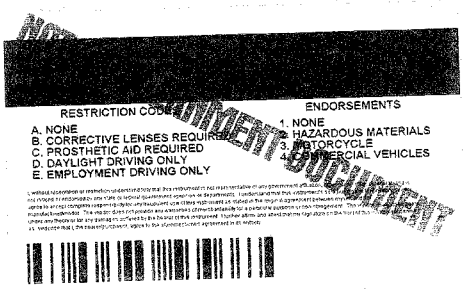
Developed under a contract with the American Health Care Association and
The Department of Health, Education and Welfare

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 9

IN PLASTIC POUCH





OUT OF PLASTIC POUCH

NOT A GOVERNMENT DOCUMENT

OKLAHOMA
NATIVE AMERICA

CLASS	NUMBER	SEX	ISSUED
C	328-42-1229	M	02-14-00

BIRTHDATE	EXPIRES	ORGAN DONOR
06-30-53	02-14-04	

WT.	HT.	EYES	REST.
180	5-11	BRN	NONE

UNDER 21 UNTIL

1496

WILSON, KEITH E.
1914 LAKE RD
PONCA CITY OK 74601

328-42-1229

[redacted]

RESTRICTION CODES

A. NONE
B. CORRECTIVE LENSES REQUIRED
C. PROSTHETIC AID REQUIRED
D. DAYLIGHT DRIVING ONLY
E. EMPLOYMENT DRIVING ONLY

ENDORSEMENTS

1. NONE
2. HAZARDOUS MATERIALS
3. MOTORCYCLE
4. COMMERCIAL VEHICLES

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 10

Hotmail *keithewilson@hotmail.com*

Inbox | Compose | Addresses | Folders | Options | Help

Inbox

From: Mexican311 REDACTED dress - Block Sender
Reply-To: "Fakeidman's ID List" <fakeidman@listbot.com>
To: fakeidman@listbot.com Save Address
Subject: HeRe wE gO
Date: Fri, 17 Mar 2000 12:55:41 EST

Reply | Reply All | Forward | Delete | Previous | Next | Close

Fakeidman's ID List - http://pages.eidosnet.co.uk/fakeidman/

ALRIGHT IM ONLY GONNA SAY THIS ONCE SO LISTEN UP. I DONT TALK ON THIS LIST BECAUSE THE LARGE MOAJORITY OF STUFF DISCUSSED IS BORING AND BULLSHIT. IM NOT INTO GETTING INTO ARGUMENTS ABOUT THIS SO BELIEVE ME IF YOU CHOOSE, BUT IF YOU DONT IT WOULD NOT BOTHER ME ONE BIT.

OK, the IDShop sends their ID in a white evelope, exactly as they describe on their webpage. 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. You can do this

OK, the IDShop sends their ID in a white evelope, exactly as they describe on their webpage. 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

reject you, you simply say that this is a State Identification Card, dont yall have them in this state? Usually they will accept them, since the ID's are of pretty good quality. The hologram is cheesy but it should still work in most areas.

One last piece of advice, The IDShop makes good ID's but they are far from flawless. You can get caught using any fake ID, but the chances raise a bit with these ID's. Now if you take my advice, remove the disclaimer on the back, you should increase your chances of not ever getting arrested. Remember, the best ID's are the ones you custom make, since you can change any details and make them exact duplicates of the real ones. But if your looking for a good ID to merely buy alcohol underage or simply get into a few nightclubs, the IDShop is well worth your money. Any other use is a bit sketchy, so good luck and follow this advice. Its the truth.

Senate Permanent Subcommittee
On Investigations
EXHIBIT # 11

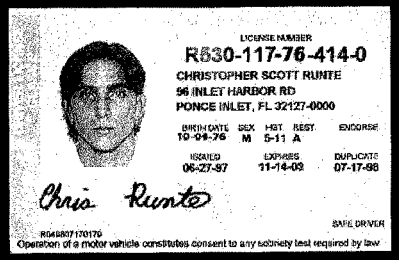
FRAUDULENT IDENTIFICATION UNIT

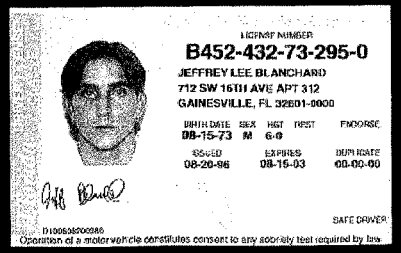
ENFORCEMENT & TRAINING

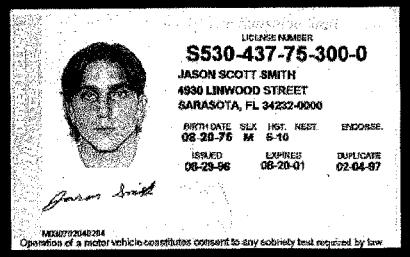
JOSEPH MARTELLI, DIRECTOR

FLORIDA DIVISION OF ALCOHOLIC BEVERAGES AND TOBACCO

THREE NAMES ARE BETTER THAN ONE







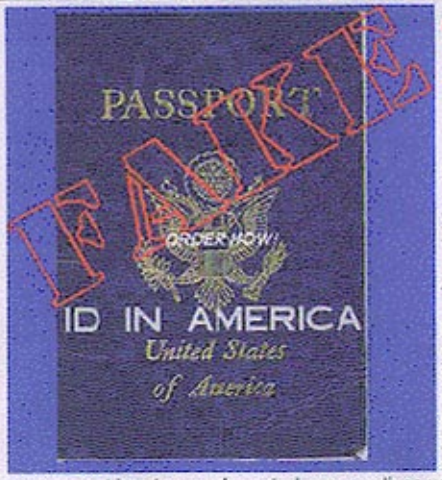
Home
Order
Gallery
Credit Cards
Feedback
FAQ
News
Disclaimer
Gallery
Arkansas
DL
SAMPLE
Georgia
YOUR
PHOTO
HERE
MISSOURI
Sample
OKLAHOMA
VISA
ORDER
NOW!
YOUR
PIC
HERE
D415-353-77-972-0
Florida

Cybernet

Fake ID In America

Home | Up | Feedback | Contents | Search | Order

Cyber3PAK | Fake ID In America | StoryBook | Available



Everything you ever wanted to know about fake ID ...

Ever wanted to disappear?

Or perhaps you are intrigued with the James Bond lifestyle?

Avoiding a stalker?

Many people use the methods we explore in "Fake ID In America" as a tool to vanish, whether it be to start over from all of the past credit problems to avoiding a stalker to even just enjoying the idea of having a multiple identity. Others feel the government has too much control over our lives with all of the computer databases they have available.

SELECT YOUR SOFTWARE TITLE
Identification The Easy Way
The Fine Art of Lock Picking
Green Thumb Plus
Advanced Breaking Games
Homemade Explosives
Identification the Easy Way, Version 2.1
CALIFORNIA
NOTE:
This is an actual
ID compiled with this software
Our biggest selling title! This software program for Windows can create EXACT replicas of real driver licenses, front and back from ALL 50 states, from ANY color printer! (Legally we must remind you that once you print the ID, you are breaking the law, however it is completely legal to own this software in computer form, as long as you don't print). Also included are Social Security cards and Birth Certificates. With this software, you will receive:
- Driver Licenses from all 50 states!
(front and backs included) (both new and old versions)
- 5 Complete Lamination Kits
(sent in the mail, even if you choose to download the software)
- 2 REAL Holograms (Peel & Stick)
(these are EXACT replicas of the real thing, from the)
(state of your choice. Coupon is sent with the kit in)
(mail, as the holograms are supplied by a different)
(company ... Holographic Enterprises. You will)
(receive this even if you download the software)
- Birth Certificates
- Social Security Cards
- Complete Instructions
- Even Make the New PVC Licenses!
This is an unbeatable offer, and currently our monthly special! This means

Fake ID Zone

OVER 100 HIGH QUALITY TEMPLATES!
GET INSTANT ACCESS USING YOUR CHECK, CREDIT CARD, OR TELEPHONE!

Everything you need to make a fake id!
All for 1 price of $14.95

Section	Description
Instructions	- Complete Step by Step Instructions To Making A Fake ID -
Templates 2	- Over 30 New High Quality Templates, Including Hard To Find U.S. Templates, And Foreign Templates, Such As Vietnam, Israel, etc... -
Templates 3	- Press ID's, Permit To Carry Concealed Weapons, State ID Cards, [illegible], Security Guard, Travel Agent, Plus More! -
ID Templates	- Drivers License Templates For All 50 States -
Resources	- Directory Of Resources For ID Holograms And Laminating Materials -
Birth Certificate Template	- Get A Whole New Identity With A New Birth Certificate -
Fake ID Make	- Program For Making Fake ID's On A Mac -
Bar Code Maker	- For Those Of You Who Need Bar Codes For Your Id's, Do It Online Easily -

Fake ID, FakeID, Fake ID, ID templates, Holograms

Page 1 of 1

+ ID ZONE +
Main Page
Information
Kit Prices
Contact Us
Members
Ultimate CD
Web Links
Online Order
Mail Order
ID Books
Make Money

Everything you need to make a novelty id! All for 1 price of $19.95

Our novelty id kit allows anyone to make a new identity. Maybe you would like to be able to spot fake id's 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 online instructions with details on how to use your kit - as well as hundreds of templates, and and tech support if needed. Prices are as low as $19.95 per a kit. We curently have 2 versions of the kit ready to order, the online kit, and the ultimate id kit on CD. Check out our information section **for more information...**

Quantity orders available - Resellers welcome - Express Shipping

Lowest prices guaranteed - If you find cheaper we will beat the price =)

(c) 1999 - Fake ID Zone - Email webmaster Now - Webmasters Earn $$$

PHOTO ID SOUVENIR CARDS
ANY STATE PROVINCE OR COUNTRY

Choose your authentic Souvenir ID card from any country.

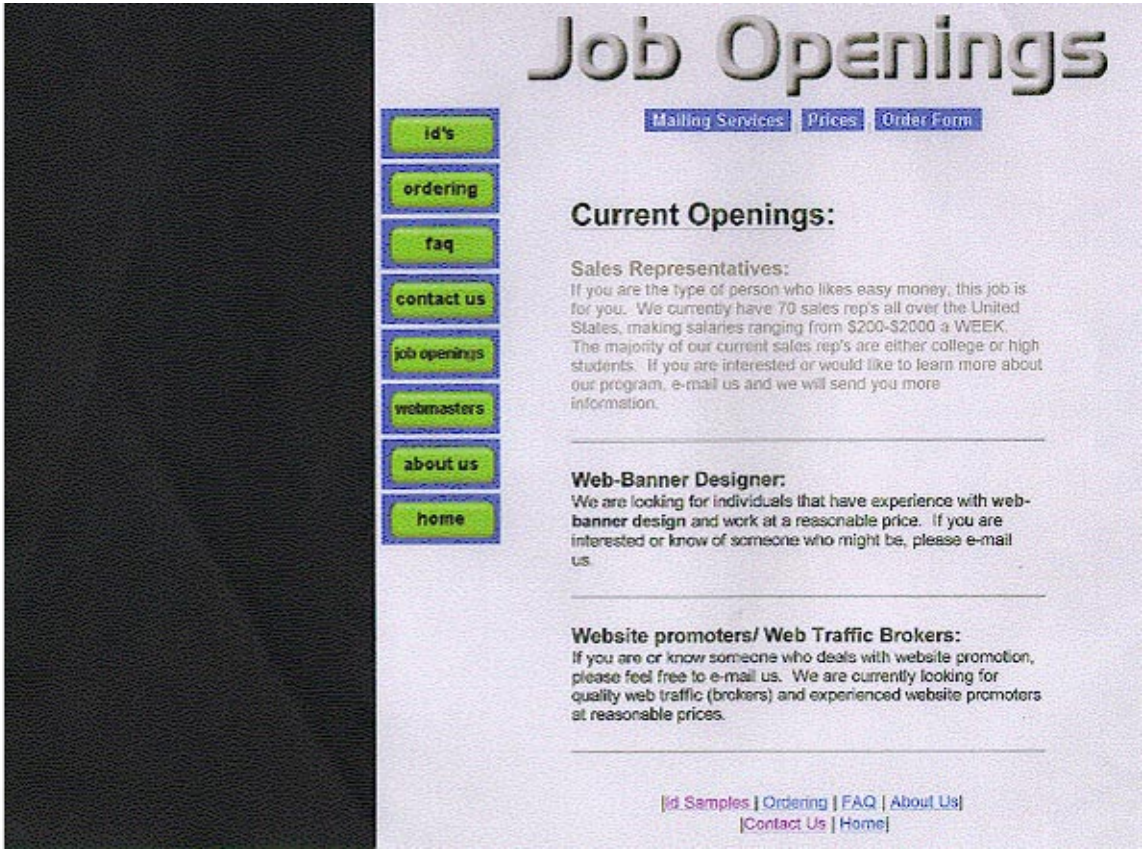
All types of Souvenir ID cards...IE: Provincial ID, State ID, International ID, Student ID, Travel ID, Press ID, FBI ID, Police ID, Social Security ID, Employment ID, Business Cards, University and College ID Cards, Birth Certificates, Award Certificates... Karate Expert, Pilot, Parachutist..DEA Agent, even a Guiness World Record Breaker... ....Thousands of ID Cards to choose from.

Protect Your Own Privacy! Become ANYONE You Want!Surprise your friends and FOOL...ANYONE...ANYTIME...ANYWHERE...
Repair your credit.....Travel in style.....Protect your loved ones.....
No one will know the TRUTH but Yourself.
Dissappear completely and Start a New Life!

- WORLD'S LARGEST SOUVENIR ID CARD MANUFACTURER & SUPPLIER
- SUPERIOR HIGH QUALITY ID CARDS WITH HARD PLASTIC LAMINATES
- ALL ID CARDS ARE PROFESSIONALLY DESIGNED BY AN EX-DMV STAFF
- 25 YEARS OF EXPERIENCE WORKING WITH DMV OFFICES WORLDWIDE
- SECURITY HOLOGRAMS AND SEALS FOR POSITIVE PROOF ANYWHERE
- CARDS ARE QUALITY CONTROLLED AND GUARANTEED TO PLEASE YOU
- A 100% GUARANTEE TO BEAT ANY COMPETITORS ADVERTISED PRICE

GET YOUR SOUVENIR ID FROM ANYWHERE IN THE WORLD

24 HOUR SECRET INFORMATION LINE


Job Openings
Mailing Services
Prices
Order Form
id's
ordering
faq
contact us
job openings
webmasters
about us
home
Current Openings:
Sales Representatives:
If you are the type of person who likes easy money, this job is for you. We currently have 70 sales rep's all over the United States, making salaries ranging from $200-$2000 a WEEK. The majority of our current sales rep's are either college or high students. If you are interested or would like to learn more about our program, e-mail us and we will send you more information.
Web-Banner Designer:
We are looking for individuals that have experience with web-banner design and work at a reasonable price. If you are interested or know of someone who might be, please e-mail us.
Website promoters/ Web Traffic Brokers:
If you are or know someone who deals with website promotion, please feel free to e-mail us. We are currently looking for quality web traffic (brokers) and experienced website promoters at reasonable prices.
|id Samples | Ordering | FAQ | About Us|
|Contact Us | Home|

The largest seller of counterfeit ID's in the U.S.
Connecticut
Virginia
HUNT, JAMES P.
16290 WOODLAND DR.
DANVILLE VA 24544
Louisiana
Fake IDs, ID cards, novelty ID holograms, photo ID, The ID Shop, fake ID
Page 1 of 2
The ID Shop.com
id's
ordering
faq
contact us
job openings
volunteers
New PVC Plastic Id's !
Holograms
Effective (10-19-99): The ID Shop will no longer accept or process orders from the State of Florida, due to the Statewide False Identification Program in Florida.
Convention in Las Vegas
defcon

FakeID.Net discussion board

- **FakeID.Net Discussion** April 16 - 09:17 am

Welcome to the new and improved FakeID.Net discussion board. If you were registered on our previous message board, it is necessary to re-register. Click on "Get Message Board ID" to obtain your free user account. Thanks, and if you have any questions, Please do not hesitate to let me know.

---

at 3:40 AM on Wed, September 23 the original User List was scrapped. This means if you received a message board ID, it is necessary to re-enter it. Board messages were NOT lost, but User account was updated, and in an effort to make this board easier to manage, was replaced with a fresh list. I am sorry for those roughly 2 dozen people affected. Hopefully this will be the first and last time something like this will happen.

Sincerely,

the Web Host (WebHost@FakeID.Net)

COUNTERFEIT ID SALES

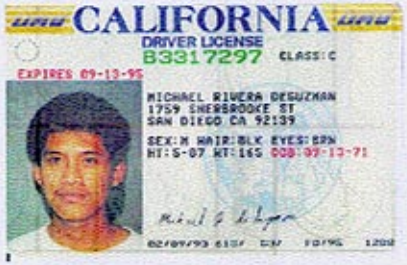
ON THE

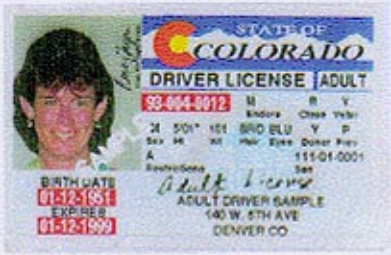
INTERNET

ISSUE
COUNTERFEIT
ARIZONA
IDENTIFICATION CARD
JOHN Q SAMPLE
SAMPLE
Organ Donor No
ARIZONA
Number
Expires 05-01-2002
Birthdate 05-01-1977
RORY Q SAUN
901 N LAKE DRIVE
MARION, AZ 85705
ARIZONA
Number
Expires 02/15/2001
Birthdate 02/15/1977
ANDRE PAZ
6500 SW 92 STREET
PHOENIX, AZ 33156
RESTRICTIONS AND ENDORSEMENTS

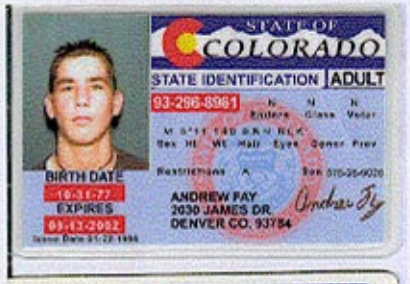
ISSUE

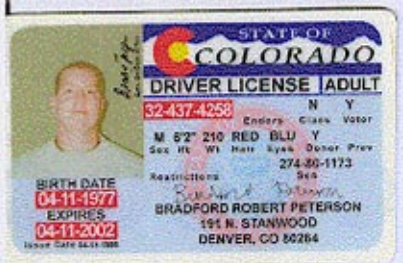
COUNTERFEIT





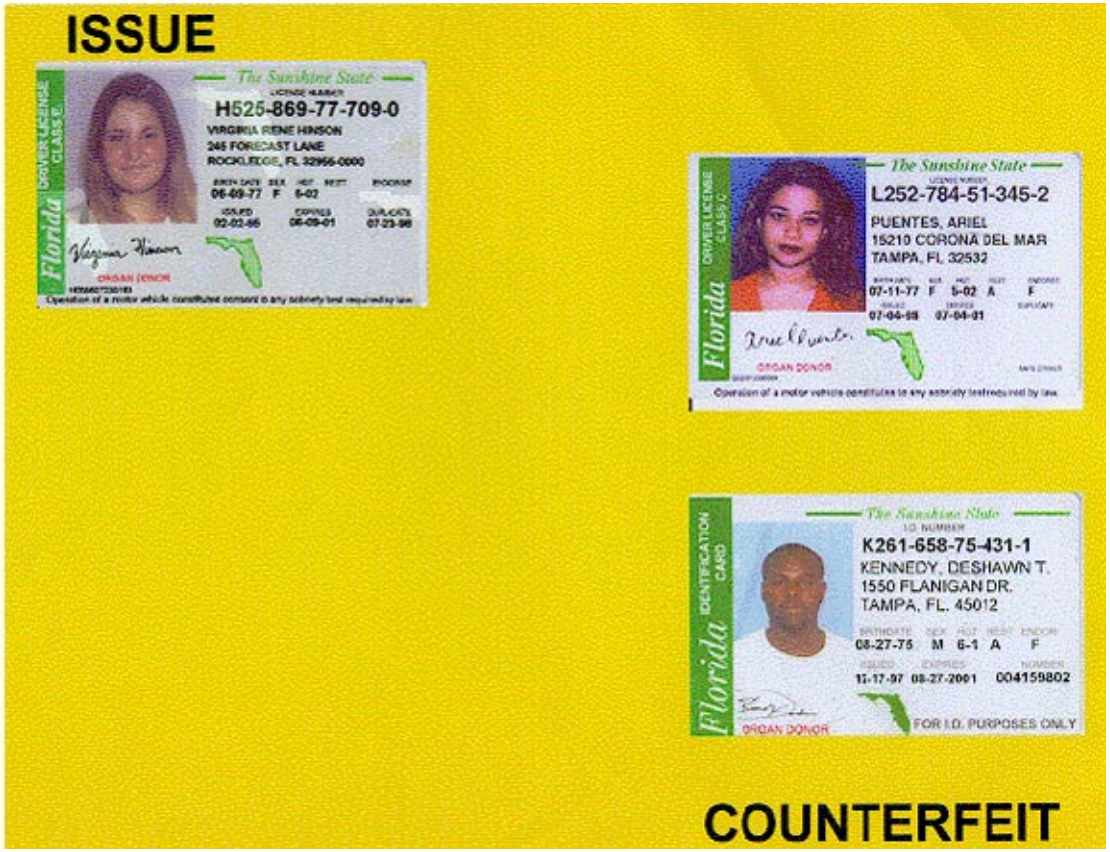
ISSUE





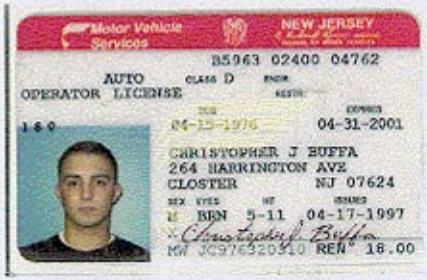
COUNTERFEIT

ISSUED
LICENSE
COUNTERFEIT
Connecticut
DRIVER'S LICENSE
026825160
DRIVER, ANY
123 ANY ST
ANYTOWN
02-02-2001
Connecticut
DRIVER'S LICENSE
026825151
02-01-98
Connecticut
DRIVER'S LICENSE
023989283
02-02-98
Connecticut
DRIVER'S LICENSE
230457360
05-27-99

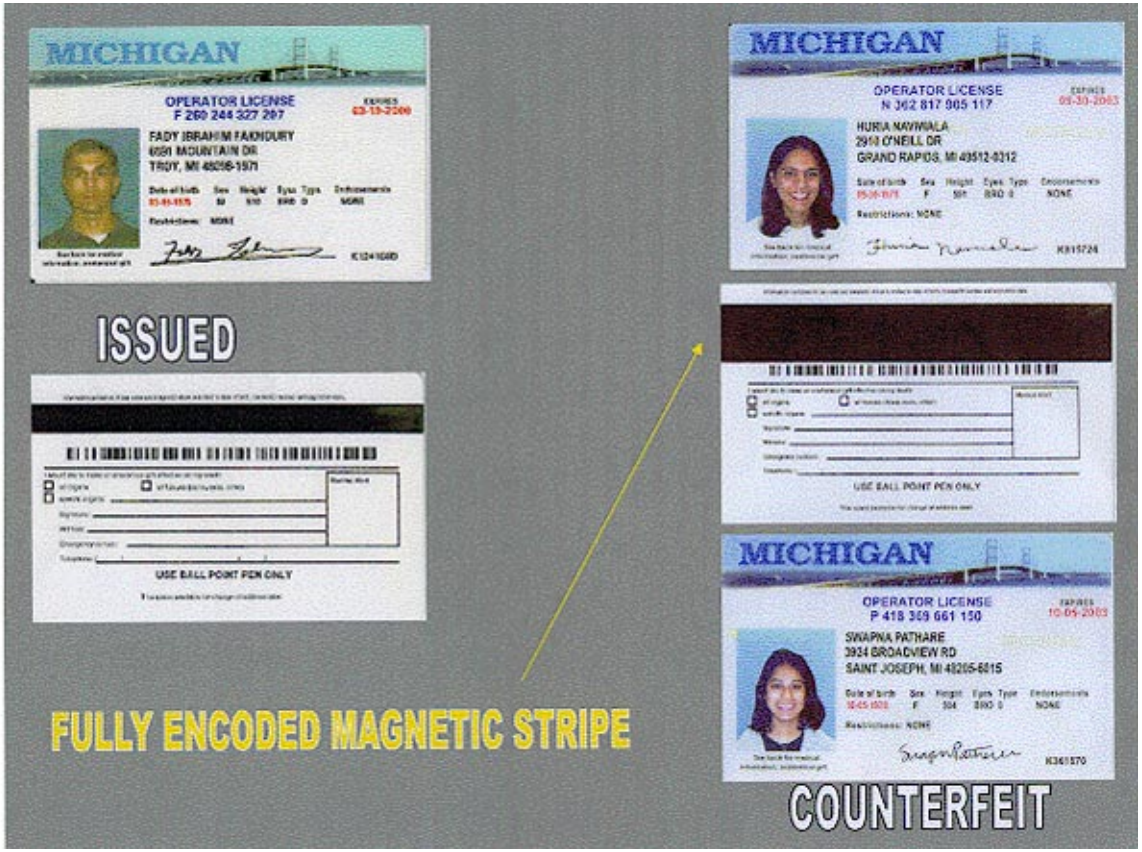

ISSUE
Florida
DRIVER LICENSE
CLASS E
The Sunshine State
H525-869-77-709-0
VIRGINIA IRENE HINSON
245 FORECAST LANE
ROCKLEDGE, FL 32966-0000
06-09-77 F 5-02
02-02-96 06-09-01 07-23-96
ORGAN DONOR
Florida
DRIVER LICENSE
CLASS C
The Sunshine State
L252-784-51-345-2
PUENTES, ARIEL
15210 CORONA DEL MAR
TAMPA, FL 32532
07-11-77 F 5-02 A F
07-04-98 07-04-01
ORGAN DONOR
Florida
IDENTIFICATION
CARD
The Sunshine State
I.D. NUMBER
K261-658-75-431-1
KENNEDY, DESHAWN T.
1550 FLANIGAN DR.
TAMPA, FL. 45012
08-27-75 M 6-1 A F
11-17-97 08-27-2001 004159802
ORGAN DONOR
FOR I.D. PURPOSES ONLY
COUNTERFEIT

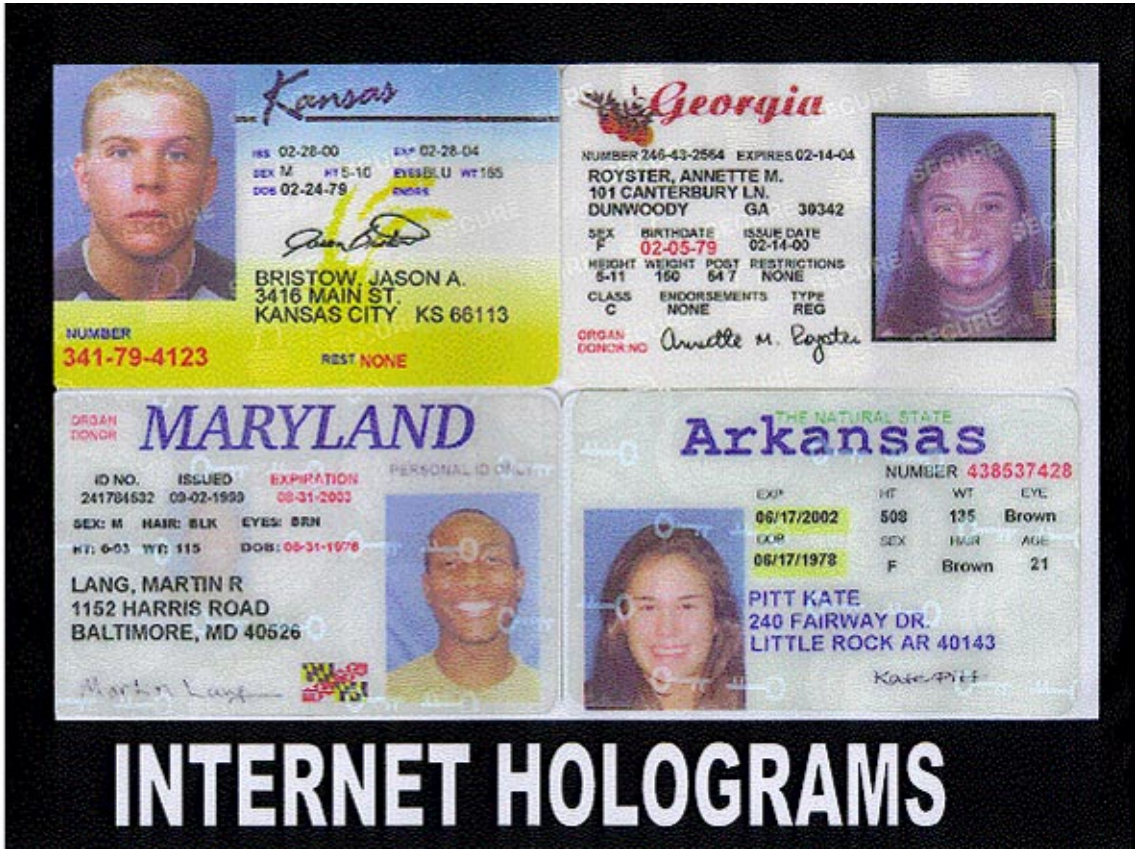
THE MOST COMMON FRAUD IN 1998-2000

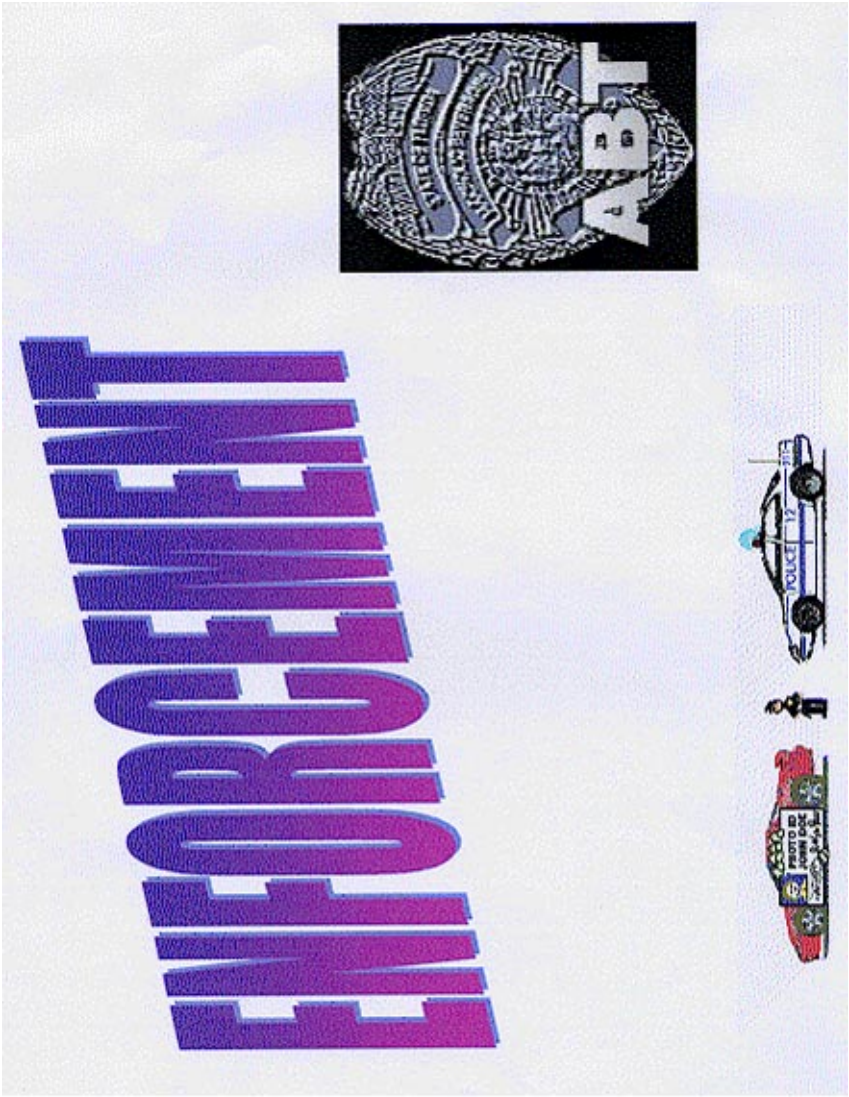
ISSUE

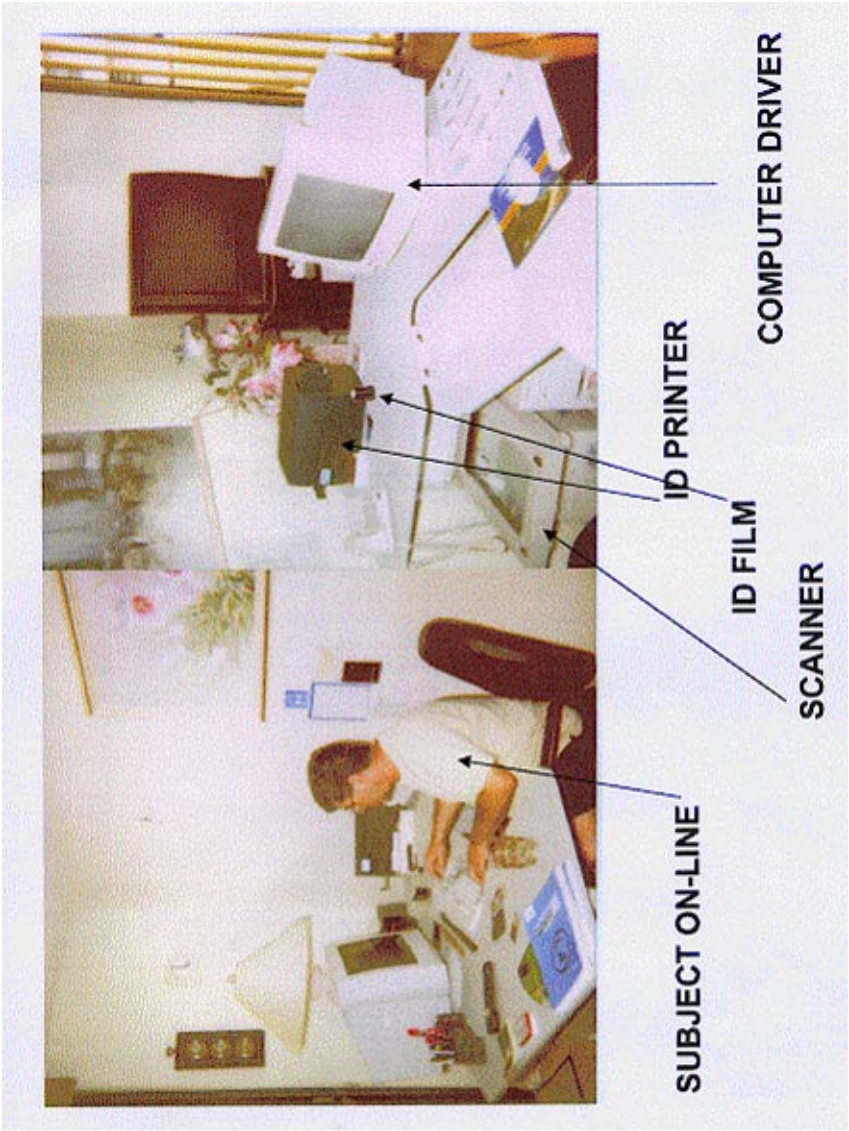


COUNTERFEIT


MICHIGAN
OPERATOR LICENSE
F 260 244 327 287
FADY IBRAHIM FAKHOURY
6091 MOUNTAIN DR
TROY, MI 48098-1971
ISSUED
USE BALL POINT PEN ONLY
FULLY ENCODED MAGNETIC STRIPE
MICHIGAN
OPERATOR LICENSE
N 362 817 905 117
HURIA NAWWALA
2910 O'NEILL DR
GRAND RAPIDS, MI 49512-0312
USE BALL POINT PEN ONLY
MICHIGAN
OPERATOR LICENSE
P 418 369 661 150
SWAPNA PATHARE
3934 BROADVIEW RD
SAINT JOSEPH, MI 49085-6815
COUNTERFEIT


Kansas
ISS 02-28-00
EXP 02-28-04
SEX M
HT 5-10
EYES BLU
WT 165
DOB 02-24-79
BRISTOW, JASON A.
3416 MAIN ST.
KANSAS CITY KS 66113
NUMBER
341-79-4123
REST NONE
Georgia
NUMBER 246-43-2564
EXPIRES 02-14-04
ROYSTER, ANNETTE M.
101 CANTERBURY LN.
DUNWOODY GA 30342
SEX
F
BIRTHDATE
02-05-79
ISSUE DATE
02-14-00
HEIGHT
5-11
WEIGHT
150
POST
54 7
RESTRICTIONS
NONE
CLASS
C
ENDORSEMENTS
NONE
TYPE
REG
ORGAN DONOR NO
MARYLAND
ORGAN DONOR
ID NO.
ISSUED
EXPIRATION
SEX: M
HAIR: BLK
EYES: BRN
DOB:
LANG, MARTIN R
1152 HARRIS ROAD
BALTIMORE, MD 40626
THE NATURAL STATE
Arkansas
NUMBER 438537428
EXP
06/17/2002
HT
508
WT
135
EYE
Brown
DOB
06/17/1978
SEX
F
HAIR
Brown
AGE
21
PITT KATE
240 FAIRWAY DR.
LITTLE ROCK AR 40143
INTERNET HOLOGRAMS


ENFORCEMENT
ABT


SUBJECT ON-LINE
SCANNER
ID FILM
ID PRINTER
COMPUTER DRIVER

MIAMI BEACH OPERATION
STATION # 1
STATION # 2
PHOTO ID
HERE

The man behind internet ID sales for:
FAKEID1, FAKEIDS, & FAKEIDONE.COM
Selling 100's of DL's & ID's a month for all 50 states.

Age 19 Home Tallahassee, Florida

ALL YOU
NEED

85 DL'S ready for mail

STATE OF NORTH CAROLINA
DRIVER LICENSE
Florida
DRIVER LICENSE
CLASS E
NEW YORK STATE
DRIVER LICENSE
NEW YORK STATE
DRIVER LICENSE

REPORT ID FRAUD

AT

idfraud@aol.com

FLORIDA ID FRAUD UNIT 904-727-5580 FAX 904-727-5559

DAVID MYERS, ID FRAUD PROGRAM COORDINATOR

Motor Vehicle Division NEW JERSEY

C5093 65564 07714

FOR IDENTIFICATION ONLY

CLASS I — EXPIRES

07-15-1971 — 04-30-2003

112

RICHARD D CLASEN
3 WILLIAM ST
OLD BRIDGE NJ 08857

SEX — EYES — HGHT — WGHT — BIRTH

M BRO 6-00 04-09-1999

LJ KB159970990483 N 6.00

Senate Permanent Subcommittee On Investigations

EXHIBIT # 12

a Control number		OMB No. 1545-0008	This information is being furnished to the Internal Revenue Service. If you are required to file a tax return, a negligence penalty or other sanction may be imposed on you if this income is taxable and you fail to report it.
b Employer identification number REDACTED		1 Wages, tips, other compensation 102000.00	2 Federal income tax withheld 28560.00
c Employer's name, address, and ZIP code CFI Electronics Corporation 1751 South 4800 West Salt Lake City, UT 84104		3 Social security wages 42700.00	4 Social security tax withheld 2144.20
		5 Medicare wages and tips 102000.00	6 Medicare tax withheld 947.32
		7 Social security tips	8 Allocated tips
d Employee's social security number REDACTED		9 Advance EIC payment	10 Dependent care benefits
e Employee's name, address, and ZIP code Richard D Clasen 3 William Street Old Bridge, NJ 08857		11 Nonqualified plans	12 Benefits included in box 1
		13 See instrs. for box 13	14 Other 0.00
		15 Statutory employee ☐ Deceased ☐ Pension plan ☐ Legal rep. ☐ Deferred compensation ☐	

16 State	Employer's state I.D. no.	17 State wages, tips, etc.	18 State income tax	19 Locality name	20 Local wages, tips, etc.	21 Local income tax
NJ		102000.00	1135.44			

Form **W-2** Wage and Tax Statement 1998 — Department of the Treasury—Internal Revenue Service

Copy C For EMPLOYEE'S RECORDS (See Notice to Employee on back of Copy B.)

CITY OF NEW BRUNSWICK

DEPARTMENT OF HEALTH -:- BUREAU OF STATISTICS № 2655

New Brunswick, N. J.

This is to Certify that the following is correctly copied from a record of Birth in my office.

DO NOT ACCEPT THIS CERTIFICATE UNLESS THE SEAL OF THE CITY IS AFFIXED HEREON.

NAME OF CHILD	SEX	PLACE OF BIRTH	DATE OF BIRTH
RICHARD DAVID CLASEN	MALE	NEW BRUNSWICK, N. J.	JULY 15, 1971

Mother: DORIS COLLINS (Maiden Name)

Father: BRUCE CLASEN

Date filed JULY 18, 1971

[SEAL]

Gloria O'Hara

Registrar of Vital Statistics

JAN 28 1982

Date of Issue

Fee $2.00

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 13

About Promastercard

Prom@ster C@rds

About Promastercard

USA Price List

World Price List

Some novelty ID's will only be created out of 2 or 3 colors, whereas the real ID has over 10 different colors. This is because it is **illegal** to re-create documents such as currency or drivers licenses of the same size AND color. So when an ID is sold a lot of the time by these novelties companies on the net, it will either be smaller then normal or have some abnormal colors in it.

Promaster Cards on the other hand operate outside the law. We are openly admitting that we are breaking State, Federal and several European law by providing ID that are exact replicas in every detail of the current IDs provide from the countries in our list

We provide matching **Driver Licenses** using PVC, Polyester and Acetate **for card material**. Our **methods of printing** are Security Micro Printing, Black Light Printing, Thermal Printing, Ultraviolet Lacquer and Top Coating.

Promaster Cards on the other hand operate outside the law. We are openly admitting that we are breaking State, Federal and several European law by providing ID that are exact replicas in every detail of the current IDs provide from the countries in our list

Product Knowledge

Every now and then we even make headline news from around the world. Here is what one news agency have to say about us: ABC from Australia.

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 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.

Before providing such a service to our internet clients, we provided fake Photo I.D. for certain elements of today's society as well as one or two PEOPLE WE COULD CARE TO MENTION. **Now**, due to the onset of internet commerce, we can now provide that service for you. We know that we are breaking the law but if you want the best counterfeit ID in the world, join the security service of Israel & Russia. If, however you want the best commercially, then you now what you have to do.

If it is a novelty card you are after so you can show off to you friends and have a laugh then this is not the place for you. However, if you on the other hand want the Photo I.D. required to become someone you are not and need exceptional quality material to do so, then this is the site for you.

To find out more then check out our sample page and our product knowledge page.

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 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.

Senate Permanent Subcommittee
On Investigations
EXHIBIT # 14

PromasterCards Ltd creased trading following the outcome of the Senate Governmental Affairs Permanent Subcmte on Investigations on:

"False ID's and the Internet"

Any orders receive will be "returned to sender"

19th May 2000

WARNING

THE FOLLOWING SITES ARE A SCAM:

www.fake-id.org
www.id-2000.net
www.false-id.net

THIS IS A MAJOR MAIL FRAUD OPERATION
WHICH HAS SEVERAL "FAKE ID" WEB SITES LISTED ON YAHOO

IF YOU SEND YOUR MONEY TO ANY OF THESE SITES ALSO KNOWN AS
UK ENTERPRISES
CDS ENTERPRISES
EIDS ENTERPRISES

YOU WILL GET NOTHING IN RETURN
THEY ARE RUN BY THE SAME PERSON

THESE COMPANIES DO NOT EXIST.

IF YOU PHONE THE NUMBERS ADVERTISED YOU WILL BE RE-ROUTED BACK TO
AN ANSWERING MACHINE IN THE U.S

THE ADDRESSES SHOWN ON THE WEB SITES ARE MAIL FORWARDING SERVICE OWNED BY
MAIL BOXES, ETC.
www.mbe.com

WHICH FORWARDS YOUR MAIL BACK TO NORTH AMERICA WHERE YOUR MONEY IS
STOLEN.

YOU HAVE BEEN WARNED

promastercards@eastmail.com

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 17

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

QUESTIONNAIRE

1. Please identify all name(s), physical location(s), mailing address(es), email address(es), domain name(s), owner(s), officer(s), and director(s) of any and all entities under or through which you provided false identification products or novelty identification products, or information about similar products, from January 1, 1999, to the present.

2. Please list and describe each product offered by entities identified in item 1.

3. Please provide three copies or samples of each product identified in item 2, in the form such products are delivered or provided to customers.

4. Please state the date(s) the entities identified in item 1 were established, and the date(s) each entity began providing false identification or novelty identification products.

5. Please state the number of orders the entities identified in item 1 received, the number of orders filled, and the gross dollar amount of sales from January 1, 1999 to the present.

6. Please state the number of employees of each entity identified in item 1.

7. Please describe the means by which the entities identified in item 1 obtained the false identification products or novelty identification products they offered. For example, if the product is a template, please explain where the template was acquired or how it was made and on what it was based.

8. Please describe the methods used to advertise, promote, or market the entities identified in item 1, and/or the products offered by those entities.

9. Please list any other companies owned or operated by any individuals identified in item 1.

10. Please list any contacts or inquiries made by any federal, state, or local law enforcement agency to any of the entities identified in item 1.

11. Please list all companies providing Internet Web hosting services for the domain names identified in item 1, and the date and a description of any instances where any domain name, Web site, or account was canceled by a Web host.

12. Please provide the name, mailing address, physical address, telephone number, and e-mail address of a representative of your company whom the Subcommittee may contact to request additional information.

✧✧✧

Received 3/27/00

WOLCOTT, RIVERS, WHEARY, BASNIGHT & KELLY, P.C.
ATTORNEYS AND COUNSELORS AT LAW
ONE COLUMBUS CENTER, SUITE 1100
VIRGINIA BEACH, VIRGINIA 23462-6765
TELEPHONE: (757)497-6633
TELECOPIER: (757)497-7267

SAMUEL W. MEEKINS, JR.

DIRECT DIAL (757) 554-0224

March 24, 2000

VIA TELECOPIER

Mr. Kirk Walder
c/o United States Senate
Permanent Subcommittee on Investigations
100 Russell Senate Office Building
Washington, D.C. 20510

Re: Answers to Questionnaire

Dear Mr. Walder:

Pursuant to your request, my client, Tim Beachum, sole proprietor of ECD which operates the bestfakeids.com website, responds to the Questionnaire you previously provided on behalf of the United States Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations. We have attempted to answer these questions as forthrightly as possible. Obviously, my client is in the business of selling novelty items on the Internet as you can see from the samples attached per your request in question number 3. We certainly hope this response satisfies your need for information from Mr. Beachum.

If you have any further questions, I would appreciate your directing them through this office. I can be reached at the numbers above.

Very cordially yours,

Samuel W. Meekins, Jr.

SWMJR/mat
Enclosures
cc: Mr. Tim Beachum (w/enc.)

TIM BEACHUM'S AND ECD'S RESPONSES TO PERMANENT SUBCOMMITTEE ON INVESTIGATIONS QUESTIONNAIRE

1. Please identify all name(s), physical location(s), mailing address(es), email address(es), domain name(s), owner(s), officer(s), and director(s) of any and all entities under or through which you provided false identification products or novelty identification products, or information about similar products, from January 1, 1999, to the present.

ANSWER:

ECD t/a Best Fake Ids
2100 Mediterranean Avenue
Box 36
Virginia Beach, VA 23451
webmaster@ecdinc.com
bestfakeids.com
Tim Beachum (proprietor)

2. Please list and describe each product offered by entities identified in item 1.

ANSWER:

I provide access to digitally formatted documentation. I do not provide actual physical documents.

Novelty driver licenses: A fictitious document, made up by me, (without an attempt to create an authentic facsimile) for each state in digital format. My site carries a disclaimer regarding use of the driver's license and the downloaded template carries a disclaimer on it saying "Not a government document," in oversized print.

Activity coordinator course completion certificate.

Birth certificate.

Press pass.

3. Please provide three copies or samples of each product identified in item 2, in the form such products are delivered or provided to customers.

ANSWER:

I do not provide a hard copy to any customer, but I have run off, for this response, an item exactly as it will come off the printer after downloading from my site.

4. Please state the date(s) the entities identified in item 1 were established, and the date(s) each entity began providing false identification or novelty identification products.

ANSWER:

My first transaction was March 17, 1999.

5. Please state the number of orders the entities identified in item 1 received, the number of orders filled, and the gross dollar amount of sales from January 1, 1999 to the present.

ANSWER:

My records indicate 1,294 orders representing sales of approximately $31,305.00. However, I previously sold other products through the web and used the same company for the financial side of the transactions and, consequently, I do not believe that all of the orders and the dollar amount set forth above constitute novelty id sales. My guess is that the novelty id portion of the orders and sales would be approximately 90%.

6. Please state the number of employees of each entity identified in item 1.

ANSWER:

No employees other than myself.

7. Please describe the means by which the entities identified in item 1 obtained the false identification products or novelty identification products they offered. For example, if the product is a template, please explain where the template was acquired or how it was made and on what it was based.

ANSWER:

Driver's license: Purchased a digital template from fakeidzone.com.

Completion certificate: I created based on scanning such a document and then altering it to make it inaccurate.

Birth Certificate: fakeidzone.com.

8. Please describe the methods used to advertise, promote, or market the entities identified in item 1, and/or the products offered by those entities.

ANSWER:

By creating my web page to cause the most "hits" from the major search engines. No other marketing.

9. Please list any other companies owned or operated by any individuals identified in item 1.

ANSWER:

None.

10. Please list any contacts or inquiries made by any federal, state or local law enforcement agency to any of the entities identified in item 1.

ANSWER:

None until this inquiry.

11. Please list all companies providing Internet Web hosting services for the domain names identified in item 1, and the date and a description of any instances where any domain name, Web site, or account was canceled by a Web host.

ANSWER:

Half Price Hosting, Louisville, Kentucky.

12. Please provide the name, mailing address, physical address, telephone number, and e-mail address of a representative of your company whom the Subcommittee may contact to request additional information.

ANSWER:

Tim Beachum.
Please see answer to number 1.

13. Please describe the past and present relationship(s) between any entity listed in item 1 and Executive Computer Designs or ECD, Inc., including but not limited to any billing, payment, or credit card processing Executive Computer Designs or EDC, Inc. performed on the behalf of any entity listed in item 1.

ANSWER:

ECD (not a corporation) has a business license in the name of Executive Computer Designs. All sales for bestfakeids.com are credit card sales and ECD has the merchant account.

14. Please describe the past and present relationship(s) between any entity listed in item 1 and Authorize.net and/or any other business providing billing or authorization services, including but not limited to identification of the business; the time frame during which the described relationship(s) existed; the type and number of credit card or other transactions the business processed on your behalf; the cumulative monetary volume of transactions; and, where applicable, the reason(s) for termination of any relationship(s) with that business.

ANSWER:

ECD's merchant account is through Authorize.net. The relationship goes back about two years but really only began to be used in the beginning of March 1999. All my transactions were through this

process and totaled, as stated in answer 5, 1,294 orders for a total amount of $31,305.00. About 90% of those were for novelty id sales.

Tim Beachum

Samuel W. Meekins, Jr.
Wolcott, Rivers, Wheary,
Basnight & Kelly, P. C.
One Columbus Center, Suite 1100
Virginia Beach, VA 23462-6765
(757)497-6633; (757)497-7267 (fax)
email: meekins@wolriv.com

WYOMING
DRIVER'S LICENSE

LICENSE NUMBER 918273645
DATE OF BIRTH 03 - 09 - 68
SEX F
HEIGHT 5' 5"
WEIGHT 125
HAIR BLK
EYES BRN
ISSUE DATE 03-09-00
EXPIRATION DATE 03-09-05
RESTRICTIONS NONE
SOCIAL SECURITY NUMBER 347 - 28 - 6844
CLASS A
SIGNATURE: _____

ELIZIBETH MCBETH G.
413 GLENNWOOD AVE.
(CITY) (STATE) (ZIP)

NOT A GOVERNMENT DOCUMENT

NOT A GOVERNMENT DOCUMENT

ALABAMA Drivers License

Alabama the Beautiful

EXPIRATION DATE 01-01-2000

JANE DOE SMITH
123 SIGNAL POINT RD
GUNTERSVILLE AL 35976

NUMBER 7791546
SEX F
DATE OF BIRTH 01-01-2000
CLASS D
ENDORSEMENT PTX
ISSUE DATE 01-01-2000
S.S. NUMBER 428-99-27-29
HGT. 5'5"
WHT. 120
EYES BRN
HAIR BLK
RESTRICTIONS A

_____

PURETO RICO

DRIVER'S LICENSE

CLASS A

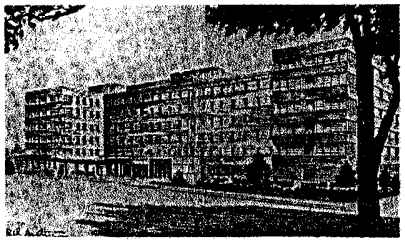
ELIZIBETH MCBETH G.
413 GLENNWOOD AVE.
(CITY) (STATE) (ZIP)

LICENSE NUMBER 918273645
DATE OF BIRTH 03 - 09 - 68
SEX F
HEIGHT 5' 5"
WEIGHT 125
HAIR BLK
EYES BRN
ISSUE DATE 03-09-00
EXPIRATION DATE 03-09-05
RESTRICTIONS NONE
SOCIAL SECURITY NUMBER 347 - 28 - 6844
SIGNATURE: _____

NOT A GOVERNMENT DOCUMENT

Victory Memorial Hospital

Waukegan, Illinois



This Certifies that _____

was born in the Victory Memorial Hospital of the City of Waukegan

on the _____ day of _____ A.D. 19____

In Witness Whereof the said Hospital has caused this Certificate to be signed by its duly authorized officer and its Corporate Seal to be hereunto affixed

_____

Administrator

_____

Attending Physician

Ohio Resident Activity Coordinator Training Project

Certificate of Attendance

IN RECOGNITION OF YOUR SATISFACTORY COMPLETION

OF THE SHORT TERM TRAINING COURSE FOR

ACTIVITIES PERSONNEL IN LONG TERM CARE FACILITIES

THIS CERTIFICATE OF ATTENDANCE IS AWARDED TO

_____

on behalf of the

American Health Care Association

Ohio Health Care Association

in cooperation with the

Association of Ohio Philanthropic Homes for the Aging

Ohio Department of Health

Ohio Therapeutic Recreation Association

at

_____

Kent State University

Certificate

_____

has successfully completed the

Nursing Home Resident Activity Coordinators Program

Presented by

the College of Special Programs

in cooperation with

the School of Home Economics
and the Gerontology Center

3.6 CEU

E02369

SCHEDULE A

Interrogatories:

1.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

2.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

3.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

4.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

5.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

6.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

7.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

8.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

9.I respectfully decline to answer on the grounds that the answer might
tend to incriminate me.

10.I respectfully decline to answer on the grounds that the answer

might tend to incriminate me.

11.I respectfully decline to answer on the grounds that the answer might tend to incriminate me.

12.I respectfully decline to answer on the grounds that the answer might tend to incriminate me.

13.I respectfully decline to answer on the grounds that the answer might tend to incriminate me.

Tim Catron
2001 W. 6th. St.
Lawrence, KS. 66044

Phone: 1-785-842-1277

Email: modsource@pitton.com

E02369

SCHEDULE B

Description of Documents:

I respectfully decline to answer, or provide documents on the grou
nds that the answer, or
documents might tend to incriminate me.

A.Manner of Objections:

I respectfully decline to answer, or provide documents on the grou
nds that the answer, or
documents might tend to incriminate me.

B.Inability to Respond:

I respectfully decline to answer on the grounds that the answer mi
ght tend to incriminate me.

Tim Catron
2001 W. 6th. St.
Lawrence, KS. 66044

Phone: 1-785-842-1277

Email: modsource@pitton.com

If you have any questions about answers given to your questions, p
lease feel free to contact:

Keith White
5030 W. 15th.
Lawrence, KS. 66049

Phone: 1-785-842-2010

1. Josh Dansereau

1775 Dax Ct

Tallahassee, FL 32308

Po Box 14348

Tallahassee, Fl 32317

Fakeidone.com

Fakeid1.com

fake-ids.com

fakeids.org

2. Business no longer in operation.

3. Business no longer in operation. Equipment donated to the state of florida.

4. April, 28 1999, business no longer in operation.

5. Business no longer in operation.

6. When business was in operation, 1.

7. When business was in operation, fargo quatro printer, PC.

8. When business was in operation, search engine.

9. None

10. Business shut down by Special Agent David Myers, Lead I.D. Fraud Investigator, Division of Alcoholic Beverages and Tobacco.

11. Not known.

12. Josh Dansereau

po box 14338

tallahassee, fl 32317

1775 dax ct

tallahassee,fl 32308

850-309-1682

FROM : www.InternetWebHosting.com PHONE NO. : 9136515012 MAR. 30 2000 02:45PM P1

JEREMY MARTINEZ
18620 HATTERAS #241
TARZANA, CA 91356

FACSIMILE TRANSMITTAL SHEET

TO: Kirk Walder	FROM: Jeremy Martinez
COMPANY: United States Senate Permanent Subcommitte on Investigations	DATE: 03/30/00
FAX NUMBER: 818-776-9958	TOTAL NO. OF PAGES INCLUDING COVER: 5
PHONE NUMBER: 818-419-7133	SENDER'S REFERENCE NUMBER: N/A
RE: Questionnaire	YOUR REFERENCE NUMBER:

☐ URGENT ☑ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

Please let me know if you need any more information or assitance in any other manner. Thanks, Jeremy

[CLICK HERE AND TYPE RETURN ADDRESS]

2/5

1)
Jeremy Martinez
18620 Hatteras #241
Tarzana, CA 91356
Newid@internetwebhosting.com

Plans.vsub.com
Newid.vsub.com
Plans.ultramailweb.com
Newid.ultramailweb.com

2) see atached

3) I deliver my product electronically via a download web site.

http://newid.ultramailweb.com

user: 898912
pass: 898912

4)
October 1999

5)Total number of orders Since January 1, 1999
1177total orders
1177 total ordes filled
Gross sales: $23,728

sales price of $19.99 between OCT 1999 and mid March 2000
sales price increased to $29.99 mid March 2000 to present

6)
no employees, just me.

7) All products are templates, which are downloaded from my website.

I obtained most of the templates by downloading them from other free websites. 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 them for free from the free sites. I started with the idea of creating and selling badges for corporations, However, I found no buyers. I then started to download these novelty ID's and found something I could actually sell. I have made some ID's myself such as the "the press ID's", which I just used my imagination to create. For instance, the "sports news" ID, I just used a cool looking font for the name of the ID, and then type press across it. The same with the "concert revue" id. The same applies to all of the industry templates which I made. The foreign templates, I just picked up off of the web. They are really bad scans rather then templates. The georiga ID I went to fakeid.net and looked at all the scans he had there. From there I used my imagination to design a template which was similar to his pictures on his free site. I did not use exact fonts, I just used the common fonts installed on windows 98 in the making of the template.

8) Advertising used to promote these items are internet search engine advertising. Where a user would go to one of the following internet search engines and perform a keyword search related to the product that I sell.

http://www.altavista.com
http://www.excite.com
http://www.infoseek.com
http://www.lycos.com
http://www.yahoo.com
http://www.dmoz.org
et. al.

9) N/A

10) Kirk Walder

11) Vsub.com (free hosting) and ultramailweb.com (freehosting)

12) See Item1

1/5

Instructions
Complete step by Step Instructinos on how to make a Fake ID!

Official Templates
Various templates including hard to find foreign templates.

Industry Templates
Permit to carry concealed weapons, State ID Cards, Militia Member, Airplane Pilot, Security Guard, Travel Agent Plus MORE!

College Dimploma
College Diplomas

Press ID's! - HOTT!

Several styles
These are hot! We have made press ID's that will get you into any concert or sporting event!! Just take a big camera and flash your new fancy PRESS PASS!

ID Templates
Drivers License Templates For All 50 States

Birth Certificate Template
Get a Whole New Identity With a New BC!

More Birth Certificates
Variastions of Birth Certificates

Fake ID Make
A Program for Making Fake ID's on a MAC!

Holograms
How To Make Holograms

Generic Bar Code Maker
For Those Of you Who Need Bar Codes For Your ID's, Do it ONLINE Easily

SSN # Verifier

This will tell you what year and which state a SSN was issued. You can simply enter numbers until you have a valid ssn! (shareware)

99 Way to Dissapear

99 Ways to Dissapear and Be FREE!

Better Ways to Dissapear

A Must have for those of you on the run!

Adobe Photoshop 5.5

Easy to use graphics program aiding you in the process of creating a fake id. (this is a DEMO version)

WinZip

Unzip files with ease. Some of our templatese are in ZIP files. (this is shareware)

FAKEID v1.0

Creates fake personal information.

Florida DL Gen

Generates DL numbers for use with Florida DL's

Illinois DL Gen

Generates DL numbers for use with Illinois DI's

Beat That Speeding Ticket

Inside tips on how to beat and avoid speeding tickets!

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 18

April 21, 2000

This affidavit is to inform the subcommittee that if I am called to give testimony before the subcommittee at a deposition , I will assert my Fifth Amendment right not to answer..

Timothy D. Gatson

Subscribed and sworn to before me this 21 day of April, 2000

NOTARY PUBLIC - State of Kansas
ADRIAN T. REEVES
My Appt. Exp. 3-11-03

Notary Public

Expires _____

KEITH A. WHITE
5030 W. 15TH ST. Suite c
Lawrence, KS 66049
785-842-2010
e-mail: constlaw@aol.com

April 21, 2000

Mr. Lee Blalack
Room 100 Russell Senate Office Building
Washington, D.C. 20510

Dear Mr. Baylock

I am representing Mr. Tim Catron before the Senate subcommittee on investigations.

I will accept service of any documents, requests or subpoenas which the subcommittee wishes to serve upon Mr. Catron.

Please contact me if you need any additional documentation for the subcommittee.

Sincerely,

Keith A. White

Keith A. White
Supreme Court # 18485

Senate Permanent Subcommittee
On Investigations

EXHIBIT # 19

AFFIDAVIT
OF
JOSH DANSEREAU

I, Josh Dansereau, being duly sworn, do depose and say as follows:

1. I reside at 1775 Dax Ct, Tallahassee, Florida 32308.

2. I have operated a Web site offering to manufacture and sell false identification, using the domain names fakeidone.com, fakeid1.com, fake-ids.com, fakeids.org, and fakeidshop.com.

3. This Web site and these domain names began operating in April of 1999.

4. I conducted my business activities using the name J and J Enterprises. I signed money orders, and made deposits to a bank account with Wakulla Bank. I was the sole employee of J and J Enterprises.

5. I made and sold a few hundred fake identification cardsbetween April and November of 1999. I received a total of approximately $3,000 to $5,000 for the identification cards I sold.

6. I used a computer program, Photo Shop, to design the identification cards to look like the driver's licenses of various states.

7. I was arrested on November 9, 1999, by David Meyers, of the State of Florida Division of Alcoholic Beverages and Tobacco. When arrested I had in my possession 85 envelopes containing identification cards that I had manufactured.

8. After my arrest, and as part of my pre-trial intervention and probation, I agreed to turn over my computer, printer and scanner, remove my Web site, cease selling and making false identification, and to return any future orders I might receive.

9. I have receive approximately 20 orders for fake identification since my arrest and have marked each of them return to sender and returned them unopened.

10. I was not aware, until my conversation on March 17, 2000 with Kirk Walder, an Investigator for the United States Senate Permanent Subcommittee on Investigations, that one of my Web sites remained on the Internet. This site, fakeids.org, was a mirror site with Webjump, that I had forgotten existed, and must have accounted for the orders I received after my arrest.

11. On April 4, 2000, after a subsequent conversation with Mr. Walder, I sent an e-mail to Webjump asking that this site be removed.

Josh Dansereau

Subscribed and sworn to before me on this 7th day of ~~April~~ June, 2000.

Notary Public
Printed Name: CAROLYN D PYE
My Commission Expires:

CAROLYN D. PYE
MY COMMISSION # CC 772665
EXPIRES: November 2, 2002
Bonded Thru Notary Public Underwriters

M:\PSI\FALSE IDs\Affidavit-Josh Dansereau.wpd

Senate Permanent Subcommittee
On Investigations
EXHIBIT # 20

STATEMENT OF
LYNNE A. HUNT
SECTION CHIEF
FINANCIAL CRIMES SECTION
FEDERAL BUREAU OF INVESTIGATION
BEFORE THE
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS
HEARING ON
INTERNET FRAUD: ILLEGAL FALSE IDENTIFICATION WEBSITES
MAY 19, 2000

Identity Theft (IDT) is not new to law enforcement. For decades fugitives have changed identities to avoid capture and check forgers have assumed the identity of others to negotiate stolen or counterfeit checks. What is new today is the pervasiveness of the problem. The Federal Bureau of Investigation does not view IDT as a separate and distinct crime problem. Rather, it sees IDT as a component of many types of crime. IDT is a common component of bank fraud, telemarketing fraud, Ponzi schemes, credit card fraud, bankruptcy fraud, intellectual property rights violations, fugitive cases, money laundering investigations, and computer crimes.

Advances in computer hardware and software, along with the growth of the Internet has significantly increased the role that IDT plays in crime. For example, the skill and time needed to produce high-quality counterfeit documents has been reduced to the point that nearly anyone can be an expert. Currently, the FBI does not compile statistics on IDT. However, by the fall of 2000, the FBI will have a system fully implemented that will track the IDT component across all white collar crime (WCC) program categories. This system will allow a manager to analyze crime trends in detail by isolating and/or combining certain crime components. For example, the system will have the ability to quickly identify all IDT cases involving the Internet regardless of the underlying crime. After the cases are identified and analyzed, managers will have the ability

to generate custom-designed reports. Equipment such as digital cameras, image scanners, high-resolution color printers, large-capacity disk drives, and laminating machines are the counterfeiter's tools of today. The same multimedia software used by professional graphic artists is now being used by criminals. Today's software allows novices to easily manipulate images and fonts, allowing them to produce high-quality counterfeit documents.

Law enforcement faces many unique challenges because of the growth of the Internet. Challenges include determining venue, identifying perpetrators, global connectivity, anonymity and ease of concealment, and the availability of information. The Internet has caused the greatest shift in the role that IDT plays in crime.

The availability of information on the Internet, in combination with the advances in computer hardware and software, makes it easier for the criminal to assume the identity of another for the purposes of committing fraud. For example, there are web-sites that offer novelty identification cards (including the hologram). After downloading the format, fonts, art work, and hologram images, the information can be easily modified to resemble a state-issued driver's license. In addition to drivers' licenses, there are web-sites that offer birth certificates, law enforcement credentials (including the FBI), and Internal Revenue Service forms.

A bank fraud case that supports the FBI's view on IDT involves fourteen victims across the United States. An unknown individual obtained three Internet access accounts using fictitious information. With stolen personal identifier information obtained via the Internet, the unknown individual applied for fourteen loans totaling more than $500,000 over the Internet. Once approved, the bank notified each loan applicant via e-mail. After receiving the approval notice for each loan application, the subject sent an e-mail to the bank requesting that the loan check be sent to an address that was different from what was stated on the loan application. The

subject needed to do this because the address given in the loan application was the true address of the fourteen people whose identities he had stolen. A number of the loan checks were successfully diverted in this manner; However, one of the checks was mailed out before the subject notified the bank to have it mailed to another address. As a result, one of the victims received a loan check in the mail along with loan papers to sign and return. The victim immediately contacted the bank and the ensuing investigation resulted in the entire scheme being uncovered. The subject was identified as Thomas W. Seitz. Mr. Seitz has pled guilty and is awaiting sentencing. During his confession, Mr. Seitz admitted to scanning in his own driver's license and altering the data. Overall, Mr. Seitz expressed his surprise at the ease with which he was able to alter data to perpetrate his fraud scheme.

There are many cases such as the one cited above. The speed with which e-commerce is growing suggests that the role of IDT across all WCC program areas will only continue to increase.

Senate Permanent Subcommittee
On Investigations
EXHIBIT # 21

Hearing on the Sale of False Identification Documents Via the Internet

Statement for the Record

Committee on Governmental Affairs
Permanent Subcommittee on Investigations

U.S. Senate

May 19, 2000

James G. Huse, Jr.
Inspector General
Social Security Administration

Madam Chair and members of the Subcommittee, I appreciate the opportunity to present this statement for the record for the Hearing on the Sale of False Identification Documents over the Internet. As you know, the Social Security Administration (SSA) Office of the Inspector General (OIG) is charged with preventing and detecting fraud, waste, and abuse in SSA programs and operations. An important part of that effort is protecting the integrity of the Social Security number (SSN) and the Social Security card, both of which are at the forefront of identity fraud issues and the crimes which follow the creation of a false identity. It is because of the importance of the SSN and of the Social Security card as an identification document that this office plays a central role in the enforcement of the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act). It is also why I felt compelled to submit this statement to the Subcommittee.

The sale of false identification documents over the Internet, particularly fraudulent Social Security cards, has quickly become a significant problem. Anyone with a computer and a credit card can obtain, almost instantly, a seemingly genuine Social Security card printed with the name and number of their choosing. This, and the purchase of similar fraudulent documents, is the first step toward establishing a new, fictitious identity, or toward assuming the identity of an existing person.

The establishment of such a false identity frequently leads to other crimes, such as credit card fraud, with a staggering impact on the economy, corporations, and private individuals.

My office is committed to using available resources to combat this problem. Despite the recency of companies profiting from the dissemination of false identification documents, my office has already taken significant steps to address this issue as part of our larger effort to combat identity fraud.

Shortly after the enactment of the Identity Theft Act, we established pilot projects in five cities with the express goal of joining with other Federal, State and local law enforcement agencies to maximize available resources to combat identity fraud. This effort has already proven to be highly successful and we are in the process of expanding to additional cities, as resources become available.

In two of the cities that have Identity Theft pilot projects, we launched an additional initiative specifically aimed at investigating the sale of Social Security cards over the Internet. Using undercover purchases of Social Security cards, Operation Dot Com, is already in the process of determining which vendors of false identification documents are in fact producing such documents, and which are merely taking money and providing no product at all. Under either scenario, our cooperative efforts with Federal, State and local authorities allows for an expanded jurisdictional approach. This permits us to take action beyond SSA program fraud, and we are already doing so in several cases. Providing details of these cases in this public forum could jeopardize our investigative effort, but we have reason to be very optimistic that we will be able to shut down several important Internet distributors of false identification documents. It is only because we already had

identity theft pilot projects in place that we were able to respond so quickly to this new Internet phenomenon.

Unfortunately, the efforts of two pilot projects represent only a drop in the bucket. While we hope to expand our efforts, and further stretch our resources by involving local authorities in our work, our primary commitment must continue to be on fraud that impacts directly on the Social Security Trust Fund. There is no question that the proliferation of fraudulent Social Security cards, like all forms of identity theft, has an impact on those programs and operations, however, it is an indirect impact. It is only when the fraudulent cards are *used* that they create errors in wage reporting and benefit payments and otherwise wreak havoc with the administration of Social Security programs. We cannot focus on the preliminary act of selling fraudulent cards to the exclusion of those cases that are draining money from the Trust Fund, nor can we ignore our other functions and our commitments to the Agency and to the American people. However, even with the limitations imposed upon us, we will continue to do everything in our power, and make the most of the cooperation of our Federal, State and local law enforcement colleagues, to confront the problem that this Subcommittee is addressing today.

To that end, I would ask that the Subcommittee consider legislative action that would aid in eliminating this illegal activity utilizing e-commerce .

Criminal laws currently on the books did not foresee, and do not adequately address, the sale of false identification documents over the Internet. For example, it is a felony under the Social Security Act to buy or sell a card that "purports to be" a Social Security card issued by the Commissioner. As you know, however, the cards sold over the Internet often carry easily removable stickers identifying them as "novelties." The difficulty in establishing fraudulent intent on the part of buyers or sellers makes prosecution of these cases problematic. Other statutes, such as sections 506 and 1028 of Title 18, which might punish those who sell or buy such cards, also carry intent requirements that make prosecutors understandably hesitant to accept these cases for prosecution. Amendment of a statute such as section 208(a)(7) of the Social Security Act, permitting fraudulent intent to be assumed from the sale or purchase of a fraudulent document, would permit at least the possibility of criminal sanctions.

Even then, overburdened United States Attorneys' Offices may not be able to prosecute such cases, which represent no immediate monetary loss to the government. I would, therefore, propose one additional remedy to this Subcommittee. Section 1140 of the Social Security Act permits my office to impose civil monetary penalties against organizations that use SSA's programs, words or symbols in advertisements in a manner that implies a connection with SSA. In recent months, we have successfully used this statute to impose penalties against, and shut down, two major nationwide direct mail solicitation companies which had been defrauding consumers through the use of SSA's good name in much the same way that the companies under review by the Subcommittee garner a profit through the unauthorized duplication of Social Security cards.

Section 1140 does not currently address Social Security card misuse, but offers a vehicle by which it *could* be addressed. By moving out of the criminal arena, and thus removing the intent element, both monetary penalties and injunctive relief could be made available. This would give us a solid means of attacking these fraud-generating companies.

Given present laws and resources, my office is doing everything possible, to eliminate the sale of fraudulent Social Security cards over the Internet, and we are pleased that the Subcommittee is aware of the gravity and scope of the problem. We would welcome the opportunity to work with the Subcommittee to close the legal loopholes that permit this conduct to continue, and to find ways to maximize those resources available to end the proliferation of fraudulent Social Security cards over the Internet.

○