S. HRG. 108–388

THE ALIAS AMONG US: THE HOMELAND SECURITY AND TERRORISM THREAT FROM DOCUMENT FRAUD, IDENTITY THEFT, AND SOCIAL SECURITY NUMBER MISUSE

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 9, 2003

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PRINTING OFFICE

92–477—PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON FINANCE

CHARLES E. GRASSLEY, Iowa, *Chairman*

ORRIN G. HATCH, Utah	MAX BAUCUS, Montana
DON NICKLES, Oklahoma	JOHN D. ROCKEFELLER IV, West Virginia
TRENT LOTT, Mississippi	TOM DASCHLE, South Dakota
OLYMPIA J. SNOWE, Maine	JOHN BREAUX, Louisiana
JON KYL, Arizona	KENT CONRAD, North Dakota
CRAIG THOMAS, Wyoming	BOB GRAHAM, Florida
RICK SANTORUM, Pennsylvania	JAMES M. JEFFORDS (I), Vermont
BILL FRIST, Tennessee	JEFF BINGAMAN, New Mexico
GORDON SMITH, Oregon	JOHN F. KERRY, Massachusetts
JIM BUNNING, Kentucky	BLANCHE L. LINCOLN, Arkansas

KOLAN DAVIS, *Staff Director and Chief Counsel*
JEFF FORBES, *Democratic Staff Director*

CONTENTS

OPENING STATEMENTS

AGENCY WITNESSES

PUBLIC WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

THE ALIAS AMONG US: THE HOMELAND SECURITY AND TERRORISM THREAT FROM DOCUMENT FRAUD, IDENTITY THEFT, AND SOCIAL SECURITY NUMBER MISUSE

TUESDAY, SEPTEMBER 9, 2003

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10:07 a.m., in room SD–50, Dirksen Senate Office Building, Hon. Charles E. Grassley (chairman of the committee) presiding.

Also present: Senators Kyl, Bunning, Baucus, and Lincoln.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM IOWA, CHAIRMAN, COMMITTEE ON FINANCE

The CHAIRMAN. I want to thank everybody for their patience and for coming to this very important hearing.

This Finance Committee oversight hearing will examine the problems of document fraud, identity theft, and Social Security number misuse. We will also look into the implications for terrorism and for homeland security.

Identity theft and document fraud is about more than just bad credit ratings or underage drinking. Identity theft and document fraud are also a threat to our national security.

Two years ago, 19 hijackers attacked our Nation in a suicide plot that killed thousands. These terrorists had lived among us, sometimes for years, leaving and entering the country repeatedly.

To plan, to plot, and carry out their mission, they needed valid identification. These hijackers used a variety of means to obtain identification, some of them even living under their very own names.

Unfortunately, getting this cover was not much of a challenge because we know that they slipped on board airplanes and turned those planes into missiles.

There are sleeper cells still lurking in this country, plotting to harm us and providing support for future attacks. Some have been arrested, some are under surveillance, and some are still at large.

Even in America's heartland, even in my own State of Iowa, document fraud, identity theft and terrorism are a concern. Law enforcement officials in Iowa are seeing more and more document fraud and identity theft.

These terrorists are alias among us, living openly, but falsely, threatening our lives and our security. Identity theft and document fraud are far too easy to commit for Americans to feel safe.

Our national security is at stake. Our government needs to do more to protect us. We have to face the fact that driver's licenses and that Social Security numbers have become the de facto national identifiers.

Without these, you cannot really function in American society. With them, you can open bank accounts, buy a gun, get a credit card, take flight lessons, and you can board airplanes.

Our government recognizes the problem of identity theft and of document fraud. But the question today is, 2 years after our attacks of 9/11, is our government doing enough about this problem? How safe are we?

How easy is it to obtain valid identity documents under an alias? How secure is the Social Security number and the driver's license process? How easy is it to make counterfeit documents that work? I do not think anyone here is going to like the answer. I do not know that I do.

We have a lot of witnesses here today to testify and to answer these questions. Before we hear from our first panel, I would call on Senator Baucus for an opening statement. After that, we will call our first panel.

Senator Baucus?

OPENING STATEMENT OF HON. MAX BAUCUS, A U.S. SENATOR FROM MONTANA

Senator BAUCUS. Thank you very much. Thank you, Mr. Chairman, for convening this hearing, particularly as we near the second anniversary of the September 11th terrorist attacks.

I think it is important to remind ourselves that, back in January, the President spoke to the Nation and reminded us about the war on terror and how high the stakes are.

In reference to the war on terrorism, he said, "As we fight this war, we will remember where it began," that is, in our own country. He further said, "We have intensified security at the border and at the ports of entry."

After the speech, this committee held a hearing to assess the security of our borders. We learned that, despite the tough talk, there were very serious questions about whether the government was doing enough.

Today's hearing focuses on another critical aspect of how we protect our homeland, the adequacy of systems used to issue identification documents to people in our country. Specifically, we will focus on the apparent ease with which an authentic driver's license can be obtained by using fictitious documents.

This committee has a vital role to play in identifying fraud through its oversight of the use of Social Security numbers. The reality is that Social Security numbers play a vital role in verifying identity.

While the Social Security Administration has taken some steps to prevent the misuse of Social Security numbers, problems still persist.

Today we will hear about two recently discovered gaps in the protection of these numbers. We also want to hear what the administration is doing, that is the Social Security Administration, to close these gaps.

But why is the issue of identification fraud important? It is worth remembering that 7 out of the 19 September 11th hijackers fraudulently obtained authentic driver's licenses through the Virginia Department of Motor Vehicles.

They used these authentic driver's licenses to board the planes on that tragic day. Even today, there are press reports that Virginia DMV workers were part of a lucrative scam that trafficked in bogus Virginia driver's licenses, and netted more than $1 million.

Last month, a man from Guinea was charged with using a false Social Security number to cash counterfeit checks as part of another conspiracy that obtained over $1.2 million.

The suspect admitted having three Virginia driver's licenses. For one, he told DMV workers he changed his name for religious reasons. For the second license, he used an international driver's license. For the third license, the DMV allowed a friend to vouch for his residency.

It remains clear that a weak link in our National security chain still exists. A driver's license is a commonly acceptable form of identification. It also plays an integral role in helping to protect our National security.

Not only are licenses used to board an airplane, they also make it possible to reenter the United States, obtain access to government buildings, open bank accounts, cash checks, and buy weapons.

What is most important about a driver's license is the apparent legitimacy it establishes. Driver's licenses, like all government-issued IDs, carry a presumption of authenticity. When we see these forms of ID, we presume the persons possessing them are who they say they are.

We lessen our suspicions, we drop our guard. We assume the government has done its job in checking out the person's credentials and has validated the person's true identity. Unfortunately, as we will hear today, this is not always the case.

GAO will tell us today that, 2 years after 9/11, many DMVs remain susceptible to fraud and abuse. The GAO will testify that DMVs are not alert to the possibility of identity fraud.

Some workers at the DMV failed to follow security procedures and report attempts to create false identities. In other cases, DMV workers told the GAO investigators what they needed to do to fix their fraudulent documents.

We will also learn that DMV offices do not have access to the appropriate information systems to fully carry out the background checks they needed to perform. In a time of heightened national security, state DMVs play an integral role in protecting us.

A driver's license is more than a license to drive. It is the primary document we use to identify ourselves. Accordingly, DMVs have responsibility to look beyond driving safety and detect counterfeit documents used to establish identity. Frankly, the DMV vulnerabilities are inexcusable.

So what are we going to do about this? First, we need better standards for issuing identity documents. This will increase detection of fictitious or fraudulent documents used to establish identity. Second, we will ensure that DMV workers are better trained to identify counterfeit documents. Third, we need more sophisticated technology at DMVs.

The Department of Homeland Security was created to facilitate communication among agencies. We also need to ensure that DMVs can communicate with each other and with law enforcement officials. Fourth, DMV workers need to become more vigilant to prevent bad actors from obtaining valid driver's licenses.

Today's hearing is very timely and disturbing. I look forward to hearing from the witnesses. I am particularly interested, though, in learning what specific steps the administration is taking to address the security weaknesses identified by our witnesses.

Talk is cheap. The American people deserve and expect action. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Baucus. You and your staff have very much cooperated with us on this hearing and other oversight hearings, and I appreciate that very much.

To start our first panel, we are going to hear from Assistant Attorney General Richard Convertino. The other witness, who is a Federal prisoner, also should be brought out just a little bit later.

Mr. Convertino is the lead Federal prosecutor in the Eastern District, Michigan. He handled the Detroit sleeper cell case. This case led to the first terrorism conviction since 9/11 and it is a flagship in the Justice Department's war on terror.

The FBI and the U.S. Attorney's office in Eastern District, Michigan did an excellent job on this case, putting three terrorists in jail and protecting our Nation.

In particular, I would like to congratulate you, Mr. Convertino, and also the other prosecutor on the case, Keith Corbett, as well as your support staff and the case agents for our FBI.

This case was a tough one, but they used an aggressive approach. It paid off with a conviction of three terrorist suspects. Mr. Convertino, I think you are a model public servant. As far as I am concerned, you should be hailed as a hero.

I have a list of your professional accomplishments, which I want to enter into the record. I think the Attorney General's words on the day of the guilty convictions are worth repeating.

Attorney General Ashcroft said, "Today's conviction sends a clear message. The Department of Justice will work diligently to detect, disrupt, and dismantle the activities of terrorist cells in the United States and abroad.

Today's verdict reaffirms our commitment to pursuing aggressively the evidence, wherever it may lead. I congratulate the prosecutors," so that would include you, Mr. Convertino, "and agents who worked tirelessly on that particular case."

I think Attorney General Ashcroft's words are right on the mark. This case began when the FBI raided an apartment in Detroit on September 17, 2001. Three suspects were arrested on document and identity fraud, a fourth suspect arrested later.

Many fraudulent documents were found in the apartment, including passports, driver's licenses, airport passes, and Social Security cards. The suspects were later indicted on terrorism charges.

Mr. Convertino is going to give us details of this case. But I can tell you that this was definitely a serious terrorist group. Three defendants were convicted in June and now are facing years behind bars. This investigation is a case study in the dangers of document and identity fraud, and how it is so connected to our terrorism problems.

Before I go any further, I also would note several issues for the record. It is unusual to have an Assistant U.S. Attorney testify before any Congressional committee. However, there is precedent for this, which I will explain.

But, first, I want to note that there are extraordinary reasons why this committee required this witness' testimony and why this committee issued a subpoena for him to testify.

No one is in a better position than Mr. Convertino to make the Congress and the public aware of the dangers of document and identity fraud and terrorism. Because of that, this committee issued a subpoena to Mr. Convertino which he was bound to obey and comply with.

Mr. Convertino is not going to tell us anything today that is not on the public record, either in court documents or news reports. He is here merely to put this all in context and explain it all to us as committee members.

Mr. Convertino is the last person who would jeopardize his own criminal case, and he will not say anything today to do that. Mr. Convertino, if you or other witnesses are asked a question by any member of this committee that may jeopardize your case, all you have to do is say so, and we will understand.

I do understand how sensitive it is to bring a line attorney before the committee. There is always the risk of politicizing a case. Nobody on this committee is more sensitive to that than I have, having served on the Judiciary Committee since my coming to the Senate.

The only time such extraordinary circumstances are warranted is when it is in the public interest to know about the threats to our own safety. The public does need to know about the dangers of document and identify fraud, and about their links to terrorism. This is clearly one of those times.

As for Congressional precedent for line attorneys to testify, I have had some involvement. In 2000, the Judiciary Committee was investigating the handling of the Peter Lee espionage case stemming from theft of nuclear secrets from our weapons labs. Line attorneys from the Justice Department were subpoenaed to testify for several of those hearings.

I also want to note that Federal law prohibits any retaliation or any discrimination against any person who testifies to the Congress. Committing those acts, I would remind everybody, is a criminal violation of 18 U.S.C., Section 1505.

I certainly do not expect there to be repercussions because Mr. Convertino is here to explain how the Justice Department is winning the war on terrorism. But just in case someone is thinking

about retaliation, this committee is not going to tolerate it. We take seriously the protection of our witnesses.

Also on the panel, is a prisoner in Federal custody who was a witness in the Detroit case. Yousseff Hmimssa plead guilty to fraud charges and was a cooperating witness for the government, and testified against terrorists.

Hmimssa became involved with a terrorist group that wanted Hmimssa to make false identity documents for them. He never did so. He never did become a full member of the terrorism cell, but he was associated with them. He can provide an inside view of how they operate and what they wanted false identity documents for.

Hmimssa was arrested in my home State of Iowa, Cedar Rapids, thanks to the good work of the Secret Service and the Cedar Rapids police department. This shows that the document fraud connections to terrorism can be anywhere, even in small communities in a rural State.

Let me also take a moment and note for the record that Hmimssa was not charged with terrorism. He was indicted on fraud charges in connection with fake documents that he made for the suspects, and he plead guilty to fraud charges, not terrorism charges.

I also understand that Hmimssa has cooperated with the prosecution, and his testimony was key for the government's victory. He has chosen to answer our questions today so that we can find out how simple it is to commit identity theft and document fraud, how simple it is to circumvent the system

On the other hand, Hmimssa is a criminal. But he is not a terrorist. He is paying, and will pay, for his crimes. He has made mistakes and he realizes that. Now he is trying to help us fix it.

Hmimssa is not on trial here today. He has agreed to help this committee. He has agreed to help the Congress and the public address the national security threat of identity theft and document fraud.

Hmimssa is not going to provide formal testimony. Instead, he will answer our questions about what he did and how he did it. He is testifying behind a screen for security reasons. Committee staff has conducted an interview with Hmimssa, and a summary of that interview will be entered into the record as an exhibit.

I would ask, without objection, that that be done at this point.

[The information appears in the appendix.]

The CHAIRMAN. Hmimssa is under tight security. I ask the audience to remain seated and quiet during this session of the hearing. We cannot have anyone come or leave at that particular time.

Mr. Convertino, we will begin with your testimony. First, I want to ask if Senator Baucus has anything to say at this point before we proceed.

After that, though, we will ask you questions. Once we finish that, the marshalls will bring Hmimssa into the room for questions.

Senator Baucus, do you have anything you want to add?

Senator BAUCUS. Yes. Thank you, Mr. Chairman.

First, while it is unusual to have an Assistant U.S. Attorney testify at a hearing such as this, these are unusual times. I commend Mr. Convertino for all his work. I think he has done a great job.

I also commend you again, Mr. Chairman. You are known for protecting Federal employees during oversight investigations, protecting Federal employees who are doing their job, and I commend you for that. This is just another case of that. I associate myself with your remarks regarding Mr. Convertino.

The CHAIRMAN. Well, thank you very much.

Mr. Convertino, would you proceed with your testimony?

STATEMENT OF RICHARD CONVERTINO, ASSISTANT U.S. ATTORNEY, EASTERN DISTRICT OF MICHIGAN, DEPARTMENT OF JUSTICE, LEAD PROSECUTOR ON THE DETROIT TERRORISM SLEEPER CELL CASE

Mr. CONVERTINO. Thank you, Mr. Chairman. Good morning.

Sir, this case started in Detroit approximately eight days after the tragic events in September of 2001, those being September 17, 2001, when members of the Joint Terrorism Task Force in Detroit attempted to locate Nabil al-Marabh. Mr. al-Marabh was the 27th person on the watch list of the FBI and they were looking to talk to him.

They went to the door, the residence at 2653 Norman Street to see if they could have a discussion with Mr. al-Marabh. He was not there. There were three defendants in the apartment, two were from Morocco and the third was from Algeria. Mr. Chairman, the Algerian defendant was acquitted of all charges at trial.

The defendants gave the JTTF members consensual search authority and they began to search the apartment. That was followed up, Mr. Chairman, by a search warrant signed by a Federal magistrate sometime in the early morning hours of September 17.

What was discovered in the apartment at 2653 Norman Street, sir, were false passports, false Social Security cards, resident alien card and visas that were false, a Day Planner that had casing sketches that I will talk about briefly in a moment, airport identification badges for two of the defendants with their names and pictures on the identification badge, a box of 105 audiocassette tapes, a casing video, a group of blank Algerian birth certificates, and dozens of passport-sized photographs were also seized.

The fourth defendant, who we believe was the cell leader, was arrested November 4, 2002 in North Carolina. Mr. Chairman, this was a Salifist Cell. The group was a radical Islamic fundamentalist group of Salifists who promoted Jihad and Holy War. The Jihad they promoted was global.

The group espoused violence against others. That is, they viewed others outside of their group as infidels. They saw the world as divided into two spheres, a zone of war, or non-Islamic area, and a zone of Islam. The United States was deemed by this group to be the zone of war.

Salifists are aligned philosophically with the Wahabis. As I am sure the committee knows, the Wahabis are aligned with Osma bin Laden.

Of the 105 tapes that were seized and introduced into evidence at trial, I have before the committee a sampling of the invective speech that was replete throughout the tapes: "oh, Allah, kill them all. Do not leave any of them alive. Oh, Allah, be without them,

whoever believe with them. Destroy them with total destruction." This is but one of the 105 tapes, sir, that were seized.

In addition to the tapes, a Day Planner was seized. The Day Planner and the false documents were deemed by the defendants to have belonged to a person by the name of Jalali.

Jalali was told to the agents by the defendants as someone who had previously lived in the apartment and had left previously. But they wanted to keep the documents, according to the defendants, in case Jalali returned. The Day Planner was one of the documents that the defendants said belonged to Jalali.

Sir, you can see on the exhibit before you, the translation of the Arabic is, "American base in Turkey under the command of the Defense Minister for all Weapons."

This was provided to the Office of Special Investigation for the Air Force in the Insurlake Air Base in Turkey. They had determined, beyond all peradventure, that this was a casing sketch of the air base in Turkey.

The expert who testified, Lieutenant Colonel Peterson, said that she believed that the planes depicted below are the three types of aircraft that take off routinely in, previously, Operation Northern Watch. The aircraft to the right depicts a fighter; in the middle, a tanker refueler; to the left, an AWACS.

The flight order which is depicted to the left of the sketch is AWACS, tanker refueler, and fighter jet. According to the expert witness, that is the exact order that those planes take off, or took off, for every operation in Northern Watch. This information was not public.

According to Lieutenant Colonel Peterson, the only way to get this information, and depicted on this sketch as accurately as it is, is having someone on the ground at the air base in Turkey.

Lieutenant Colonel Peterson believes that the lines crossing in front of the planes are possible fields of fire by shoulder-held missiles, which is a threat at that air base.

There is a factory just outside of the air base. The testimony at trial was that the experts believed that the vantage point that the person who drew this sketch was taken from this factory.

Also in the Day Planner, Mr. Chairman, were sketches that were determined by an expert in Iman, Jordan, Ray Smith, who is the Regional Security Officer at the U.S. Embassy in Jordan, to be a depiction of the Queen Alial Military Hospital in Iman, Jordan.

The words depicted on this are interpretations of the Arabic. In particular, I draw your attention to the "behind, back parking, private, non-direct." The military hospital does, indeed, have a parking lot that is behind it, as depicted here, and does have political members as patients from time to time.

A videotape was also seized at the time of the search warrant. A line bar was put together by the expert, Special Agent Paul George, who testified on tradecraft in the trial. The videotape was deceptive in its appearance, Mr. Chairman. It had on its labeling, "La Prince." It appeared, by its nature, to be a store-bought tape.

The tape was punched out so it could be re-recorded over. It was, curiously, shot and recorded over several times. You can see that the dates are out of sequence from L.A., Disney Land, Las Vegas, and New York.

If one were to put this tape in a VCR here in the United States, the only thing that they would see was fuzz. Special Agent George testified that it is in the European format, or was in the European format, and that was a way to disguise and deceive the person who reviewed the tape into thinking that the tape was blank, when in fact it had what Special Agent George testified to, was casing material of Las Vegas, Los Angeles, and New York.

At the end of the tape is a segment from an Egyptian television show. That is where the tape was when it was played first. Special Agent George said that that was because, if somebody played that in the tape, maybe someone through the Customs Service at the time the tape was tried to be taken in or out of the country, they did have the European format VCR, they could see, or would see, that it was nothing more than Egyptian television, and pass it on.

In the tape, Mr. Chairman, the photographer in the video shows a ride at Disney Land. It shows the ride and the line, going through the queue of the line. Special Agent George testified that was to show that it was a very crowded ride.

It was the only ride at Disney Land that was underground, and there was particular attention paid to the garbage cans, the trash receptacles, during the course of the line through the ride. There were no videos of the rides themselves, just this one line.

In addition, there is an outdoor scene where the translation of the videographer, they point to a water area and the person filming it says, "Here is a rising cemetery. For who? Sacrifices. We will give them to America." There is an expletive. "Strike them and throw them here. Oh, God. These sissies. How they all look." That was on the segment of the tape, Mr. Chairman, that was filmed in Disney Land.

The Las Vegas and the New York segments are equally as curious. The New York segment is from a hotel room and it zooms in on the front entranceway to the New York Times, comes back, and goes back onto the entranceway of the New York Times and the surrounding area.

In particular, the L.A. segment tracks a car from the balcony, as if one would be engaged in sniper activity from that balcony. So, it gives the perspective, it gives everything that anyone would want who is interested in casing these particular areas.

During the course of the trial, Mr. Chairman, we had closing argument, a Power Point presentation, only a part of which is here today because of time, obviously. But these were intended to corroborate the testify of Yousseff Hmimssa, who testified at length during the trial.

Mr. Hmimssa testified that one of the defendants, the Algerian defendant who was acquitted at trial, talked about blank documents and talked about filling in blank foreign documents, and turning those blank documents into legitimate United States documents.

During the course of the search, there were a group of blank Algerian documents that were seized in the house in the belongings of the defendant who was from Algeria.

The process to recruit Mr. Hmimssa and his expertise into the group occurred sometime in June of 2001, when Mr. Hmimssa moved to Dearborn and became acquainted with the defendants at

a coffee shop. The defendants invited Mr. Hmimssa to live with them.

During the time that he did, they learned that Mr. Hmimssa was an expert with the computer. Mr. Hmimssa could create false documents, which was very important to them.

They had told Mr. Hmimssa that they wanted false documents, including driver's licenses, false passports, Social Security cards so they could acquire weaponry and send this weaponry abroad to the Ikwan, or the brother, so they could set up drop boxes, so they could use and train anonymously. They had a shared hatred for the Hashemite Kingdom of Jordan and the United States, as relayed by Mr. Hmimssa at trial.

During the course of the discussion with the defendants when he lived with them, they had spoken as if they had been to Jordan. They said that they had despised Turkey and Saudi Arabia because of the presence of U.S. troops in the Islamic countries.

They referred to Las Vegas, Mr. Chairman, as the City of Satan, and spoke of Las Vegas as a prime target for attack because of the heavy tourist population.

They wanted to acquire CDL licenses in Michigan. This was an effort to acquire and transport hazardous materials. In fact, there was evidence at trial that one of the defendants told Mr. Hmimssa that he wanted to locate a truck that he could take hazardous material and drive it into the stadium in downtown Michigan.

They told Mr. Hmimssa repeatedly that they followed the Fatwas, or religious dictations of Sheik Rocman, who was convicted in the first World Trade Center bombing, and Osama bin Laden.

They justified the killing of innocent civilians based upon their being in the zone of war. This was all relayed to Mr. Hmimssa during the period of time when he lived with the defendants, Mr. Chairman. They talked about acquiring shoulder-held missiles to shoot down airplanes.

The cell leader, as I mentioned earlier, was the person who was arrested 11/4/2002, Abdulla el-Mardoudi. Mr. el-Mardoudi is a lawyer, in fact, from Morocco. He taught the defendants code.

He was able, Mr. el-Mardoudi, to make international connections and calls that were virtually untraceable. He instructed the defendants to canvass the Detroit airport for security breaches.

He told the defendants that he wanted them to have access to the planes and asked them if they could falsify documentation, including airport badges.

The defendants spoke to Mr. Hmimssa about having access to planes and getting weapons, and even a person, on board an aircraft at the Detroit Metropolitan Airport.

The cell leader, Mr. el-Mardoudi, had asked Mr. Hmimssa to create false airport badges, as well as false FBI identification. Mr. el-Mardoudi had access to funds and contacts internationally. There was evidence at trial, Mr. Chairman, that Mr. el-Mardoudi had received and sent wire transfers all over the world.

In fact, Mr. el-Mardoudi had traveled to Turkey, which was very important to tie in the Turkish air base out of the Day Planner. The Day Planner, incidentally, was obviously fingerprinted by the FBI lab. The fingerprints that came back positive were all of the defendants'.

The one fingerprint that was not found anywhere on the Day Planner, Mr. Chairman, was that of Yousseff Hmimssa, the person who the defendants initially said possessed and owned the Day Planner.

Mr. el-Mardoudi's fingerprints were on the Day Planner. On the page depicting the air base, Defendant Karim Koubriti's, who was convicted at trial, his fingerprints were on that page.

Mr. Chairman, during the course of the search, agents discovered the Michigan "CDL Answers" on both the green and the yellow forms. Those answers were discovered in and among the belongings of both of the defendants who were convicted at trial.

During the time that Mr. Hmimssa had contact with the cell leader and Karim Koubriti, they both spoke of a portion of Turkey that spoke Arabic. Mr. Hmimssa was incredulous, believing at the time that there was no area in Turkey where Arabic was spoken.

Mr. Hmimssa told the jury that Mr. el-Mardoudi told him that there was a city that he had traveled to that was very close to the border of Syria called Anatokya. Hmimssa testified that Mr. el-Mardoudi told him he traveled there to meet with Ikwan, or like-minded brothers.

Among the documents that were seized from Mr. el-Mardoudi when he was arrested, and also from a storage locker in Cedar Rapids, were documents that the Turkish terrorism unit tied into having been used as aliases for travel into Turkey on at least three occasions. Those were Hussein Hussan Sofadin, and Abdul ela-Naji.

The testimony at trial showed that persons by that name and using that identification had been into Turkey on more than one occasion.

Mr. Hmimssa testified that he received his foreign passports and the passports that were used by him to alter and be altered from the defendant, el-Mardoudi. At the time of Mr. el-Mardoudi's arrest, the agents from the DEA seized almost $90,000 in cash and money orders, three passports, 12 blank I–94 forms, a false driver's license, Salifist papers that tied back into the papers that were seized, Mr. Chairman, in Dearborn. These are but some of the items that were seized in the belongings of Mr. el-Mardoudi at the time of his arrest.

Mr. Chairman, many of the defendants' activities and methods were perfectly consistent with the al Qaeda manual that was seized in Great Britain. This came out at trial through the expert testimony of Special Agent Paul George.

This case exposed the methodology and the operations consistent with terrorist cells that have established a foothold here in the United States and have shown their ability to adopt and modify their operations.

The importance, in my mind, of this prosecution is that it engaged, it investigated, and it charged and convicted a pre-operational terrorist cell before they struck or before they could assist others in any attack here in the United States or abroad.

Finally, Mr. Chairman, I beg your indulgence to commend the other people who were involved in this case and worked tirelessly throughout the case since it began in September of 2001.

I would like to commend, personally, Special Agent James Brennan of the FBI, Special Agent Paul George of the FBI, Special

Agent Mike Thomas of the FBI, Special Agent Matt Meyer of the FBI, Special Agent Mark Pilot of the INS, Keith Corbett, my co-counsel and the chief of the Organized Crime Strike Force in Detroit, and the most important person in the case, Anna Bruny, who was the legal secretary involved and worked nonstop from the inception of this case.

So, thank you, Mr. Chairman. I am happy to answer any questions that I can.

The CHAIRMAN. We will have 5-minute rounds. I would ask the Clerk to set the clock.

Mr. Convertino, what is the importance of false identity documents for terrorists, and what did these terrorists in Detroit specifically want to use false identity documents for?

Mr. CONVERTINO. Well, Mr. Chairman, as is in the case with anyone with criminal intent, hiding one's identity can insulate and protect the subject of the criminality. In particular, the defendants in Detroit wanted false documents to travel anonymously, obtain drop boxes so they could receive and send shipments.

They wanted to train with weapons at a firing range anonymously. And, most importantly, they wanted to bring brothers, or Ikwan, into the United States anonymously as well under a false identity.

Mr. el-Mardoudi, as was pointed out earlier, did travel anonymously or under false identification to Turkey on more than one occasion. We know he has received and sent wire transfers in other names on more than one occasion.

In fact, he received a wire transfer of $1,200 on July 16, 2001 under the name of Nassim Hilali in Detroit, Michigan in order to give that money that he received to Yousseff Hmimssa to buy supplies and products so that Yousseff Hmimssa can continue on and create further false identity for Mr. el-Mardoudi and others. So, there are a plethora of reasons. The only limiting factor, seemingly, is one's imagination.

The CHAIRMAN. Was there misleading or false identify information in the Day Planner found in the terrorists' apartments?

Mr. CONVERTINO. There was what Special Agent George characterized as a security plan built into the possible discovery of the Day Planner. That is the use of a mentally incompetent person by the name of Ali Muhammad ali-Akhmed, who signed several of the pages in the Day Planner at the direction of the defendants.

Mr. Ali Muhammad ali-Akhmed was severely mentally incompetent and was cared for by his brother and his father. According to the testimony of his brother, he was unable to function on his own. In fact, the only thing he could do was sign his name and he would do anything for a cigarette.

There were also other witnesses during the course of the trial that came forward and testified who also were mentally incompetent who were sought out by the defendants and who were asked to sign onto various documents in order to protect the defendants if those documents were discovered, as was the defense at trial that the Day Planner belonged to someone who was just jotting down incoherent notes.

So, the defense was built in, expertly, I think, during the course of the use of the documents, and the people who were sought out to obtain false documents for the defendants.

The CHAIRMAN. What types of equipment were used to create false documents in this specific case?

Mr. CONVERTINO. Mr. Chairman, probably the best person to answer that would be Yousseff Hmimssa. But I am aware, through the testimony at trial, that very simple things were used to create very accurate and very good false documentation.

Mr. Hmimssa purchased items at Wal-Mart, Office Max, that kind of place to make what would appear to be very convincing false documentation that were, in fact, very passable, to the point of using those documents to travel and receive other legitimate documentations.

The CHAIRMAN. How many aliases and bank accounts did the cell leader have?

Mr. CONVERTINO. We have no idea, Mr. Chairman. There would just be too many to count. We only know of a very small number.

The CHAIRMAN. How did the defendants communicate among themselves and with other terrorists?

Mr. CONVERTINO. The cell leader, el-Mardoudi, had become very proficient at what is known as shoulder surfing, or stealing phone card numbers from people at airports. He would pass those phone card numbers on, and then the defendants and others would use those phone cards to call switching stations in Europe.

So if defendant one wanted to contact defendant two and they are one apartment away in the same town, the would call through Mr. el-Mardoudi, Europe, Western Europe, and could travel all over through the European continent and come back to that very apartment right next door and be totally untraceable. That was the testimony at trial.

The CHAIRMAN. This will be my last question, then Senator Baucus will ask.

What was the impact when authorities discovered the Day Planner sketches at the Turkish air base? And I would like to have you describe how the sketches were accurate, or how you knew they were accurate.

Mr. CONVERTINO. I knew they were accurate in my own mind, because I went to Turkey and I want to Iman, Jordan. I, along with Special Agent Mike Thomas, were able to compare the sketches in the Day Planner with what we saw.

We went and climbed a rope to the top of that factory, both of us, along with the Air Force personnel, and were able to hold copies of what we had from the Day Planner and oversee the air base, and had a clear and unobstructed view of the airplanes, of their take-off pattern, of the hardened bunker that Lieutenant Colonel Peterson said is depicted on the Day Planner in the lower corner.

Special Agent Thomas testified about what he personally observed while he was in Turkey and while he was in Iman, Jordan regarding those particular sites, as well as experts from both of those countries.

And to answer your first question, the operations group commander for Operation Northern Watch revised the flight approach

and the departure to counter any possible shoulder-fired missile attacks, as a result of having received copies of the Day Planner.

The CHAIRMAN. All right.

Senator Baucus?

Senator BAUCUS. Thank you, Mr. Chairman.

Mr. Convertino, what authentic documents are most easily obtained through forged readers? Would it be driver's licenses, would it be Social Security, would it be airport workers' passes, would it be government ID? Which ones are the legitimate ones that are the ones most easily obtained based on fraudulent information?

Mr. CONVERTINO. Senator Baucus, Mr. Hmimssa would be a better witness than I to tell you exactly what types of documents might be easier to obtain. I can tell you that the documents that he obtained and that were obtained fraudulently and falsely in our trial ran the gamut, from driver's licenses, to Social Security cards, to passports, to visas, to resident alien cards. All of those documents were created falsely and brought in as evidence in our trial, and they were very passable.

Senator BAUCUS. I understand he may be a better witness. That is, he probably is closer to the action, if you will. But, still, based on your experience and based on your knowledge, which are more easily obtainable?

Mr. CONVERTINO. Well, I recall how easy it was for Mr. Hmimssa to acquire all of those documents that were admitted into evidence and to transform a legitimate document by the use of something as common as Photo Shop, which is purchased at any large department store.

So, he was able to use Photo Shop and move, amend, and manipulate what he had on a scanner or had scanned into his computer, then quite easily adjusted what he had through the use of Photo Shop and other computer programs that he manipulated to make very, very passable false documents.

Senator BAUCUS. Now, you must have given a lot of thought to all this. That is, how easy it is to get authentic ID based on fraudulent documents. What is the best solution? It seems like it is pretty easy to do and it is pretty easy to get some authentic IDs based on fraudulent documents. What do we do about this? How do we control it? Where do we start?

Mr. CONVERTINO. Senator, that is several levels above my pay grade. I am sorry, I do not feel competent to answer that question.

Senator BAUCUS. But you must have some sense. Just, gosh, you see these driver's licenses, you see these passports. You see all of these various IDs, and at some point you probably think, gosh, I want to prosecute this case and I want to win, and I am going to win. But at the same time, you must be thinking, gosh, we have got to figure out some way to prevent some of this.

Mr. CONVERTINO. Well, the only thing I can tell you, Senator, with certainty, is when I have a case that has false identification, and I have had others, my sole goal is to be able to prove that the identification is false beyond a reasonable doubt at the time of trial. That is where my brainstorming stops.

Senator BAUCUS. Why is Mr. Hmimssa making himself available here? I would think that it creates certain risks for him.

Mr. CONVERTINO. I think it does. Mr. Hmimssa has been extraordinarily cooperative since the time he and his attorney decided to come forward. He has fully divulged his criminal activities, known and unknown, to the government. He has been very forthcoming.

I think his attitude—and he can certainly tell you better than I—is that this is activity that he was engaged in. He is not proud of it. He is not happy about it. If he can do anything to attempt to turn that around, I think he is prepared to do that. I think that is, in sum and substance, what his attitude is now, Senator.

Senator BAUCUS. All right. We can certainly ask him. But if he one in that category who sees the world in two camps, somewhat black and white, I am a little bit surprised to find him so cooperative.

Mr. CONVERTINO. He has been.

Senator BAUCUS. You trust his statements?

Mr. CONVERTINO. I very rarely trust anyone's statements, Senator. What I can tell you is, you can see on the screen, where it says "corroboration of use of Hmimssa," that was a large part of our case, quite frankly.

The information that Mr. Hmimssa told us had to most definitely be corroborated and accepted by the jury in order to be believable to the point that they would vote to convict the defendants.

So, that was our main goal, is to take his statements and corroborate them. We were able to do that on about 20 different occasions, including just the few that were shown.

I will give you one example, if I may. I spoke of the wire transfer that was received in Dearborn on July 16, 2001 for approximately $1,200. Mr. Hmimssa told Mr. el-Mardoudi, the cell leader, that he needed to acquire a printer, he needed to acquire some supplies, and he needed to acquire the products in order to create good, passable, false documents.

Mr. el-Mardoudi made a telephone call, instructed someone in Amsterdam to wire funds under the name Nassim. That was what Mr. Hmimssa told us. The only word that he recalls is "Nassim."

A subpoena was issued. The information that came back that was presented at trial was that there was a wire transfer on that particular day for the amount that Mr. Hmimssa previously said he recalled under the name Nassim Hilali.

Now, at the time the defendant was arrested, Mr. el-Mardoudi, it was November 4, 2002, several months after this information was divulged to us. On his person, Mr. el-Mardoudi, was false identification in the name of Nassim Hilali.

That is on this document before you here today. He had the very Social Security card, the resident alien card that he used. Mr. Hmimssa would have no way of knowing what he would have on him or if he would have anything on him at the time he was arrested.

Senator BAUCUS. My time has expired. Thank you very much.

Mr. CONVERTINO. Thank you, sir.

The CHAIRMAN. Thank you, Senator Baucus.

Now, Senator Bunning?

Senator BUNNING. Thank you, Mr. Chairman. I am very, very interested in the false identification on Social Security numbers, par-

ticularly. I will wait until the expert witness on identity theft comes forward.

My question to you is, if in fact this gentleman who was the cell leader was involved, when did you prosecute this case?

Mr. CONVERTINO. This year, in June.

Senator BUNNING. In 2003.

Mr. CONVERTINO. Yes, sir.

Senator BUNNING. And when did you incarcerate or capture the three or four people in the cell, other than the leader?

Mr. CONVERTINO. September 17, 2001.

Senator BUNNING. September 17, 2001.

Can you give me some idea why it took you until 11/4/02 to find the cell leader and capture him?

Mr. CONVERTINO. I can tell you that he was a fugitive and that we did not even know his name. We knew his first name, that was relayed to us by Mr. Hmimssa, as Abdullah. We had no idea what his name was.

He was arrested with a plethora of false identification under various names. You can see on the screen, his picture is on two. It is on a resident alien card and also on a New Jersey driver's license under two separate names. He flitted and floated in the United States under aliases for a long time.

Senator BUNNING. Was there any evidence discovered during your investigation that might indicate that there were active cells that were also associated with a cell that you discovered and prosecuted?

Mr. CONVERTINO. No, sir.

Senator BUNNING. None?

Mr. CONVERTINO. No, sir.

Senator BUNNING. In other words, there were only four people in the cell and you were successful in prosecuting three?

Mr. CONVERTINO. Actually, with Mr. Hmimssa, it would be four. Mr. Hmimssa would be convicted as well.

Senator BUNNING. But he was not convicted as a terrorist.

Mr. CONVERTINO. Yes. That is right, sir. He was not.

Senator BUNNING. In other words, there were three that were convicted as terrorist and one that was——

Mr. CONVERTINO. Acquitted.

Senator BUNNING. And one that was acquitted completely?

Mr. CONVERTINO. Yes, sir.

Senator BUNNING. I have no more questions.

The CHAIRMAN. Thank you. I will go back to Senator Baucus. Otherwise, I just had one question before we bring in Mr. Hmimssa.

Do you have another question?

Senator BAUCUS. Yes. I am just curious if you know, Mr. Convertino, how many terrorists have been convicted in the U.S. since 9/11?

Mr. CONVERTINO. I do not know, Senator. I do not know how many individuals have been convicted of terrorism-related charges since that time. I just do not have that information.

Senator BAUCUS. All right. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Yes. One last question about Mr. Hmimssa before we bring him in.

Could you describe the plea agreement that Mr. Hmimssa entered into with the government and the extent of his cooperation with you?

Mr. CONVERTINO. Well, as I mentioned, Mr. Chairman, I think his cooperation was extraordinary, up to and including today. The plea agreement outlines charges, I believe approximately a dozen charges or so that Mr. Hmimssa had plead guilty to, in three different districts, including Chicago, the Northern District of Illinois, Cedar Rapids, and the Eastern District of Michigan. He plead guilty to all of the charges that were brought against him in all three districts.

In return for that, he is receiving a downward departure for his acceptance of responsibility, which is, under the guidelines, a three basis point reduction. He is looking at approximately 46 months. But he has not been sentenced as of yet. He awaits sentencing, as do the other defendants.

The CHAIRMAN. All right. I thank you.

Now, I reminded everybody that when we bring Mr. Hmimssa in that nobody can leave or enter the room during this phase of the hearing. Cameras will have to be turned off and pointed down while he comes in.

Would we bring in Mr. Hmimssa at this point, then?

[The summary of the Senate Finance Committee interview with Yousseff Hmimssa appears in the appendix.]

Mr. Hmimssa, I thank you for agreeing to be here today. We are going to ask you some questions about your involvement in the case and how you made false identity documents. I am going to ask questions for five to seven minutes, and then I would turn it over to Senator Baucus, if he has questions, then other Senators that want to be involved in this.

Mr. Hmimssa, thank you for cooperating with the committee.

Would you please describe the process by which you would create a false identity for a person residing illegally in the country?

STATEMENT OF YOUSSEFF HMIMSSA

Mr. HMIMSSA. First of all, I need a passport. Then, using the passport, a foreign passport, I need a visa. There is a sticker that I am going to put on the visa and have this person go and apply for a Social Security card at the Social Security Administration.

Once they get the card in the mail, within, like, 10 days, they will get the card, along with the passport, and go and apply for a driver's license or ID at the Secretary of State.

The CHAIRMAN. All right. When you came to the United States, and I believe that was in 1994, how did you gain entry into the country and how did you get the documents that you needed to enter the United States?

Mr. HMIMSSA. I was living in Europe, so I bought a French passport and I came to the United States as a French citizen. So I got here and went to Chicago in 1994 and I was, at that time, here legally. Then I went and I applied for a Social Security card. I got it in the mail. I went and I applied for a driver's license and ID.

Senator BAUCUS. Sir, how did you get your French passport?

Mr. HMIMSSA. I bought the French passport from the black market in Europe.

Senator BAUCUS. Thank you.

The CHAIRMAN. Did you finish your statement on my second question?

Mr. HMIMSSA. Yes, sir, I did.

The CHAIRMAN. All right.

Once you got here, what documents did you get to establish yourself in Chicago, and how did you get those documents?

Mr. HMIMSSA. As I said, I got to the United States using the French passport. Once I got to the country, I went to the Social Security Administration and I applied for a Social Security card. I applied for it. Within 10 days, I got it in the mail. Using that card, along with the passport, I went to the Secretary of State in Illinois and I got ID and a driver's license.

The CHAIRMAN. Can you explain in more detail how you got your Social Security number? It is my understanding that you got that Social Security number under the name of Patrick Vuillaume.

Mr. HMIMSSA. Yes, sir, that is right. Patrick Vuillaume. The passport, as I said, I bought from the black market, which was another fake passport. The only thing that is not fake is my picture on it. The name, the number, everything is fake. So, it is under the name Patrick Vuillaume.

The CHAIRMAN. All right.

Could you explain in detail how you got the Illinois driver's license under that same name?

Mr. HMIMSSA. Yes, sir. Once I got to the country, under Patrick Vuillaume, using the French passport, I went to the Social Security Administration and I applied for a Social Security card. I was asked some questions. I answered those questions. After 10 days, I got a Social Security card in the mail.

I took the Social Security card, the one I got in the mail, with my passport and a document or a form that is called an I–94 to the Secretary of State in Illinois, and I got ID done. I went and I took the exam, the driving test and writing test. I passed and I got an Illinois driver's license under the name Patrick Vuillaume.

The CHAIRMAN. All right.

Then how did you, further, obtain a license to drive a taxi?

Mr. HMIMSSA. I went to college and took classes, all under Patrick Vuillaume. I went to the City of Chicago and took the exam, the driving exam, and I passed that exam and got a license.

The CHAIRMAN. And it is my understanding you also were able to open a banking account. How about that?

Mr. HMIMSSA. Yes, sir. Yes. Under Patrick Vuillaume, I opened a bank account in Chicago.

The CHAIRMAN. How did you receive educational training under the names that you used?

Mr. HMIMSSA. I just went to the college, it was all under Patrick Vuillaume, and I took classes. So, that was the name I was using the whole time.

The CHAIRMAN. All right.

Please explain the process for how you obtained a genuine U.S. passport under the name of Edgardo Colon. Is that right?

Mr. HMIMSSA. Yes. Edgardo Colon.

The CHAIRMAN. How did you get a passport under yet another name?

Mr. HMIMSSA. Yes. When I was staying in Chicago for over 3 years, I wanted to go back home to see my family, so I went to get a passport. I could not use the French passport, so I bought an American birth certificate and Social Security card from the black market, from someone who was able to give me those documents for some money.

So, using those documents, the birth certificate and Social Security card, under a different name, I went to the Secretary of State and I got an ID and driver's license using that ID, along with the birth certificate. I went to the post office and I applied for a passport, and I got it in the mail after a few days, 10 days.

The CHAIRMAN. So then you got an Illinois driver's license again, under the name of Edgardo Colon.

Mr. HMIMSSA. Yes.

The CHAIRMAN. Then that, in turn, was used to get the passport.

Mr. HMIMSSA. Yes, sir.

The CHAIRMAN. What happened that made you stop using the passport under the name of Edgardo Colon?

Mr. HMIMSSA. I paid taxes under this name. I was trying to live under this name, because it is legal. It is a passport, you know. It is like living like a citizen. I paid taxes under this name.

Then I got a letter from the IRS that said the Social Security number that you paid taxes with was used by another taxpayer. So, obviously the person who sold me the document was still using his number.

The CHAIRMAN. What is the importance of the I–94 form, and what did you do with these forms?

Mr. HMIMSSA. With the I–94, I was able to create a blank I–94 using the computer, scanner, and a printer. With that document, along with the passport and visa, I would go to the Social Security Administration and apply for a Social Security card, or send someone to apply for a Social Security card.

The CHAIRMAN. My time is up now. So, Senator Baucus?

Senator BAUCUS. Thank you, Mr. Chairman.

Mr. Hmimssa, you said you obtained your French passport on the black market, and you have used the black market a couple of times here.

How big is the black market? How easy is it to get documents on the black market so you do not have to forge them or counterfeit them, you can go out and buy them?

Mr. HMIMSSA. Here in the United States or overseas?

Senator BAUCUS. I want to you to answer both questions, both the United States and overseas.

Mr. HMIMSSA. Well, overseas, it is really easy. If you have the right connections, you can get any passport, French, Italian, or any passport from Europe.

Senator BAUCUS. And in the United States?

Mr. HMIMSSA. The same thing. You just have to have the right connection. You can get birth certificates, you can get Social Security cards of someone who is not using them, or someone dead.

Senator BAUCUS. Which authentic IDs are most easily obtained through counterfeit documents? Would it be a driver's license? What would it be?

Mr. HMIMSSA. First of all, you have to have the right document to get the driver's license, the Social Security card and the birth certificate. But for a foreigner, a Social Security card and a passport. That is really easy to get.

Senator BAUCUS. Is it easy to get a Social Security card?

Mr. HMIMSSA. Yes. It is very easy.

Senator BAUCUS. It is very easy to get a Social Security card.

Mr. HMIMSSA. Yes.

Senator BAUCUS. You said when you applied you were asked some questions. What were those questions?

Mr. HMIMSSA. Just simple questions, like the date of birth, mother's maiden name, father's name. That is all.

Senator BAUCUS. How do you add security features, such as holograms, watermarks and reflective inks?

Mr. HMIMSSA. With the I–94, the INS, it has got, like, some security feature on it. Once you put it under UV light, it shines. The fake one does not shine. So, some offices have this kind of technology and they verify the I–94 under UV lights. So, if it is fake, it will not shine. The ink will not shine if it is not.

Senator BAUCUS. How easy is it to counterfeit?

Mr. HMIMSSA. I was able to do that, too.

Senator BAUCUS. Watermarks, all of that? The ink, and so forth.

Mr. HMIMSSA. The ink. Yes, I was able to do that. I was able to come up with the ink that would shine under a UV light.

Senator BAUCUS. Now, do you consider yourself an expert, the best in the field, or are there a lot of other people who could do the same thing?

Mr. HMIMSSA. There are a lot of people out there who can do more than I, who are more expert than I.

Senator BAUCUS. What about other IDs, like for airport employees? Have you ever attempted to make documents, counterfeit those documents?

Mr. HMIMSSA. I was asked to make such documents, airport badges and FBI identification cards, but I never did that.

Senator BAUCUS. Do you think you could make a false FBI identification card?

Mr. HMIMSSA. It is very easy.

Senator BAUCUS. Very easy.

Mr. HMIMSSA. Yes.

Senator BAUCUS. In your own words, why is it so easy?

Mr. HMIMSSA. All you have to do, is you have to have an FBI identification card. You scan it. You remove the name and you put in a new name, and you print it.

Senator BAUCUS. And that would be true for most any document?

Mr. HMIMSSA. Yes.

Senator BAUCUS. Now, if, say, the President of the United States were to ask you, Mr. Hmimssa, I need your help in stopping this, what would some of your suggestions be to make it more difficult to get false documents, false IDs?

Mr. HMIMSSA. Something like a smart chip that is used in Europe, with fingerprints.

Senator BAUCUS. Fingerprints.
Mr. HMIMSSA. Online fingerprints.
Senator BAUCUS. I am sorry. What is a smart check? What is that?
Mr. HMIMSSA. A smart chip. They use it like a smart card.
Senator BAUCUS. I see.
Mr. HMIMSSA. It is a microchip which can be found on credit cards, can be found on IDs and driver's licenses in Europe, in some countries in Europe.
Senator BAUCUS. All right.
Anything else come to mind?
Mr. HMIMSSA. As I said, fingerprints.
Senator BAUCUS. Fingerprints.
Mr. HMIMSSA. Eyes.
Senator BAUCUS. Eyes. Eye prints.
Mr. HMIMSSA. Yes. Could be voice recognition.
Senator BAUCUS. Voice recognition, perhaps.
But hearing you, it sounds like it is pretty open here in the United States today. It is pretty easy to make false IDs. Would that be a correct or incorrect statement?
Mr. HMIMSSA. It is all over the world, sir.
Senator BAUCUS. Well, thank you.
This is very alarming, Mr. Chairman.
Have you noticed the government cracking down? Is it harder now, more difficult today than it might have been a couple, 3 years ago to make false IDs without apprehension?
Mr. HMIMSSA. I do not know. I have been in custody for 2 years, so I do not know what is going on outside.
Senator BAUCUS. Is there a network? Do you talk to fellow people? You are a lone ranger. You just do your own operation. Is that right? In fact, you are not part of a team that counterfeits. You just counterfeit for your close associates.
Mr. HMIMSSA. Yes.
Senator BAUCUS. All right.
Thank you, Mr. Chairman.
The CHAIRMAN. Thank you.
The Senator from Kentucky.
Senator BUNNING. Thank you, Mr. Chairman.
I want to go back to how you got here. You said you had bought French passports on the black market in Europe.
Mr. HMIMSSA. Yes, sir.
Senator BUNNING. What kind of passport was it, a regular passport? In other words, there is more than one kind of passport.
Mr. HMIMSSA. There is a diplomatic passport and a regular passport.
Senator BUNNING. Yes. Well, yours was a regular one?
Mr. HMIMSSA. Yes, sir.
Senator BUNNING. What kind of visa did you get, also?
Mr. HMIMSSA. I did not need a visa. For all western countries, you do not need a visa between each other. Traveling is free.
Senator BUNNING. What about work permits?
Mr. HMIMSSA. I did not need a work permit.
Senator BUNNING. You did not need one with the kind of passport you had?

Mr. HMIMSSA. No, sir.

Senator BUNNING. In other words, your passport allowed you to come to the United States and work as a citizen might?

Mr. HMIMSSA. No, sir.

Senator BUNNING. Well, explain to me.

Mr. HMIMSSA. Well, I got to the United States and I got a Social Security card.

Senator BUNNING. I want to get back to that in a moment, because that is my hang-up. But your passport allowed you to apply for a Social Security card.

Mr. HMIMSSA. Yes

Senator BUNNING. And when you applied for the Social Security card, the questions you filled out—and as chairman of the Social Security Subcommittee over in the House, I know exactly the form that you had to fill out. So you had to falsify your mother's maiden name, and all the other things were falsified also, correct?

Mr. HMIMSSA. No, sir.

Senator BUNNING. Correct?

Mr. HMIMSSA. No, sir. I did not falsify my mother's maiden name or my father's name. I gave the information, like on the passport. But when it came to mother's maiden name and father's name, I did not.

Senator BUNNING. Well, how could your mother's and father's name be different than the passport you came in on?

Mr. HMIMSSA. On the French passport, it did not say the mother's maiden name.

Senator BUNNING. All right. But your personal name was on the passport correctly, the false name?

Mr. HMIMSSA. Yes, Patrick Vuillaume.

Senator BUNNING. And so when you applied for the Social Security card, you used the false name. Then you filled in the document, applying for the Social Security number, with a false mother's maiden name.

Mr. HMIMSSA. Yes. It did not say anything, so I gave a different mother's maiden name. I gave them my real mother's maiden name.

Senator BUNNING. We tried very hard to change the rules at the Social Security Administration that you would never have gotten a Social Security number had some of the changes we asked for gone in.

The fact of the matter is, your suggestion of a chip or a fingerprint has been suggested to the Social Security Administration for the last 10 years that I know of, and none of the advice has been taken.

We are going to have to pass a law to make it work that requires them to use chips for identification, and also to use fingerprints on the document that they send in to get a Social Security card.

Once you get the Social Security card, the whole identity for you opens up.

Mr. HMIMSSA. Yes.

Senator BUNNING. You can go to work, you can get a driver's license, you can do everything else. So, the Social Security card is the key card in getting other false documents, correct?

Mr. HMIMSSA. That is right.

Senator BUNNING. So maybe my good chairman is listening very closely to that, that the Social Security card is the key for falsification of all other documents.

So, we have got to make it a heck of a lot tougher on the Social Security Administration to make sure that illegal aliens that come into this country with black market passports are not able to just apply to the Social Security Administration and get a Social Security number because once that has happened, then they can falsify all other documents.

The CHAIRMAN. I think, Senator Bunning, it is a sad commentary for me to say. I think we have known that for a long time. Maybe it takes this hearing, plus everything else that has happened over the 2 years, to wake up to that.

In our next panel, we will have a chance to ask our own government officials the extent to which they consider that as serious as what you just said, and whether or not any actions are being taken accordingly. Obviously, if there are not actions taken accordingly, you and I would have a responsibility to make sure that those actions do take place.

Senator BUNNING. Thank you, Mr. Chairman.

One other question. In your association with this cell, these members, there were only four other people involved?

Mr. HMIMSSA. Yes.

Senator BUNNING. Never more? No stragglers that would come in and leave? Only four people involved that you lived with?

Mr. HMIMSSA. Yes, sir.

Senator BUNNING. Four.

You were captured and incarcerated quite a bit before the cell leader, then.

Mr. HMIMSSA. That is right.

Senator BUNNING. All right. Thank you very much for your testimony.

Mr. HMIMSSA. You are welcome.

The CHAIRMAN. Mr. Convertino, is there any clarification on his being a cell member or associating with the cells that needs to be clarified based upon the question that Senator Bunning asked?

Mr. CONVERTINO. Mr. Hmimssa disassociated himself with the members of the Detroit cell soon after he became aware of their activities and their desires, and moved out of the apartment within a month.

In fact, when he was notified by the cell leader at one point in time after the initial defendants were arrested to destroy everything that he had in his possession regarding false documentation, instead of doing such, which would have been easy for Mr. Hmimssa to do, he took all of the documents that he had, the fraudulently and falsely created documents that were created by him and also by Mr. el-Mardoudi, and placed them in a storage locker in Cedar Rapids. The results of that were that they were seized and used as evidence against the other defendants.

The CHAIRMAN. All right.

I have one last question, then we will go on to the next panel. This is to you, Mr. Hmimssa.

Did you use the name Colon and the passport that was associated with it to travel, and did you have any problems at ports of entry?

Mr. HMIMSSA. Yes, sir. I used the passport under the Colon, Edgardo, which was an American passport, to travel to Morocco, and came back. I did not have any problems.

The CHAIRMAN. All right.

Just before the panel leaves, I just wondered, is there anything that you should add, Mr. Convertino, at this point that we have not asked you, or in regard to anything that Mr. Hmimssa said?

Mr. CONVERTINO. Not that I can think of. Thank you, Mr. Chairman.

The CHAIRMAN. All right.

I want to thank both of you very much for testifying and answering questions. Mr. Convertino, I think this committee has really learned something about the dangers of identity fraud and terrorism, and what is at stake.

You also showed that the government can put people who do this sort of thing behind bars. You did an excellent job on the case and I am sure your U.S. Attorney, Mr. Collins, and the Attorney General are proud of the victory that you brought in this case.

Mr. Hmimssa, I thank you for testifying here. You did not have to do this. You chose to cooperate, and that is very much appreciated. Your information also will help this committee understand the problems of identity and document fraud.

You have evidence of considerable talents in this area. I hope you put them to really good use, not illegal use, when you are released.

You both are excused, and I thank you for coming. I would tell everybody, as Mr. Hmimssa leaves the room, stay seated until he is gone, and would ask that all cameras be turned off and pointed down.

We will have a brief recess while Mr. Hmimssa leaves. Thank you. Mr. Convertino, I thank you for coming, too.

[Pause]

The CHAIRMAN. Now I would like to introduce our second panel. After that, our last two witnesses will testify and answer questions.

First, I would like to introduce Mr. Asa Hutchinson, Undersecretary for Border and Transportation Security of the Department of Homeland Security.

Many of our security problems highlighted by the General Accounting Office fall under Mr. Hutchinson's jurisdiction, so we are going to look forward to hearing what he has done to shore things up.

Mr. Hutchinson, I appreciate very much your coming to the table.

Next, we have Mr. Robert Cramer of the General Accounting Office's Office of Special Investigations. He is here to deliver his report. He will be accompanied by Mr. John Cooney and Mr. Ron Malfi, who will answer questions. Mr. Cramer will testify about a new report that shows how easy it is to get valid driver's licenses under aliases.

The General Accounting Office also has information about how document fraud revealed major security problems in our govern-

ment, at our borders, airports, gun stores, and sensitive Federal buildings, including weapon depots.

We also have Mr. James Lockhart, the Deputy Commissioner of Social Security. Mr. Lockhart will discuss what his agency is doing to protect Social Security numbers, and hopefully how it is working with the Department of Motor Vehicles of the various States in the driver's license process.

I am glad to see the FBI is here today to be recognized for what it is doing in the war on terror. The FBI's primary responsibility now is counterterrorism, so it is also involved in identity theft and document fraud.

We will hear from Mr. John Pistole, the Acting Assistant Director of Counterterrorism; last, we will hear from the Inspector's Office at the Social Security Administration, which serves as both the internal watchdog and the law enforcement arm.

Mr. Pat O'Carroll, the Assistant Inspector General for Criminal Investigation, will tell us about what his office is doing to meet the challenges of ensuring the Social Security numbers' integrity. I think he will also demonstrate for us how simple document fraud can be.

I have asked that each of you keep your testimony to 5 minutes. You can submit a longer statement for the record.

We are going to start with Mr. Hutchinson. But I have, as normally is the case, when there is a report to be given by the General Accounting Office, we would allow them some extra time.

So, Mr. Hutchinson, thank you very much for coming. I know you have changed your schedule to be here for this very important hearing, and I thank you for doing that and cooperating with the committee.

STATEMENT OF HON. ASA HUTCHINSON, UNDERSECRETARY FOR BORDER AND TRANSPORTATION SECURITY, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. HUTCHINSON. Thank you, Mr. Chairman. I am grateful for the opportunity to talk about the problem of document fraud.

Clearly, the sophistication of forgers and their technology, and the increasing use of document fraud, combined, is one of the greatest challenges we face in fighting terrorism.

This year, our Customs and Border Protection inspectors intercepted over 60,000 fraudulent documents at our 300 ports of entry. The problem, of course, is the volume of acceptable documents that can be used for identification purposes.

I think one question I know that you are addressing in this hearing is, well, what can be done? And obviously it is important that individual citizens take appropriate steps to protect their own identity and the documents that they have and rely upon for identification purposes.

Second, though, I think it is important that we as a society review our entry requirements. Whenever you look at the fact that, presently, there are 240 different types of driver's licenses from the various States that can be used for entry documents for U.S. citizens coming back to the United States if they travel to the western hemisphere.

I think it is very significant that Congress has mandated that we have machine-readable passports that will reduce the reliance simply upon a driver's license or documents that can be easily forged.

The third thing that I think is important, is that we reduce our reliance upon documents as the exclusive means of identification purposes. That is one of the reasons that the Department of Homeland Security, in accordance with Congressional mandate, is working very diligently to implement the U.S. visit program that would give us the capability to take biometrics from those people that enter and exit our country. If we can track our foreign visitors through biometrics, that will reduce the reliance upon simple documents for identification purposes.

If you look, in addition, at the actions, the Department of Homeland Security training is a critical part of the protection, the training that we have for our inspectors.

The fact that Secretary Ridge took the step of unifying our inspection forces will help us and increase our ability to properly train our inspectors.

Now, Agriculture inspectors, Customs inspectors, Immigration inspectors will all be unified and their training will be enhanced at the border. We will also train the secondary inspectors to receive more advanced training on document fraud identification.

Second, the Bureau of Immigration and Customs Enforcement, or ICE, has a very aggressive forensic document lab that gives real-time assistance for the inspectors in the field, provides alerts to the field. Two of those alerts are demonstrated on the blow-ups for the committee to look at.

One of them involved an alert referencing stolen blank Filipino passports. The second one is information on counterfeit in-series passports that were available in Turkey for $500 each. So, these are information circulars to our inspectors to help identify fraudulent travel documents.

We have trained over 6,400 enforcement officials around the world in more expertise and document fraud detection.

Second, our investigations are a critical part of it. Through an initiative with the U.S. Attorney's Office in the Eastern District of Virginia, we have joined with the FBI, Social Security, IRS, Department of State, the Postal Service, the Virginia DMV, and others to investigate large immigration, visa, and identification fraud.

Here in the Washington, DC area, we have had an investigation called Operation Card Shark that goes after the counterfeit of documents in the Adams-Morgan area. To date, we have identified four document mills that have been closed, and the seizure of close to 2,000 documents with an estimated street value of $155,000. Fifty aliens have been taken into custody, 30 have been removed, and 15 have been prosecuted. One has been sentenced for 52 months.

In addition, I am very pleased with the initiative of the Bureau of Customs and Border Protection that has developed an image storage retrieval system which is a web-based system that provides 40 ports of entry with access to actually the documents that the alien relies upon, such as the alien registration card, employment authorization documents, advance parole for Adjustment of Status forms that are issued by the Bureau of Citizenship and Immigration Services.

So, those documents are entered and are available to the inspectors to compare with the document that the person is actually presenting to see if there is a disparity there. This will be rolled out in the next fiscal year.

Finally, the Secret Service takes the lead in identity theft, and they are doing an outstanding job. As a part of the team at Homeland Security, they have developed a video/CD-rom that is available as a resource for local and State law enforcement officers that they can use in combatting identity crime. All of this is more specifically outlined in my written testimony that I will offer for the record.

Thank you, Mr. Chairman, for addressing this serious problem that poses a threat to our society, the integrity of our system, and our efforts against terrorism. Thank you.

The CHAIRMAN. Thank you, Mr. Hutchinson.

[The prepared statement of Mr. Hutchinson appears in the appendix.]

The CHAIRMAN. Now, Mr. Cramer?

STATEMENT OF ROBERT CRAMER, MANAGING DIRECTOR, OFFICE OF SPECIAL INVESTIGATIONS; ACCOMPANIED BY JOHN COONEY, ASSISTANT DIRECTOR, OFFICE OF SPECIAL INVESTIGATIONS, AND RON MALFI, DIRECTOR, OFFICE OF SPECIAL INVESTIGATIONS, U.S. GENERAL ACCOUNTING OFFICE, WASHINGTON, DC

Mr. CRAMER. Good morning, Mr. Chairman. Thank you for the opportunity to summarize today some of the work which the Office of Special Investigations has performed over the past 3 years which demonstrates security vulnerabilities that exist because counterfeit identification can be easily produced and used to create fraudulent identities.

These tests revealed security weaknesses at Federal buildings and other facilities, at airports, and at our Nation's borders. They also exposed identity fraud vulnerabilities in the Social Security number application process and in the administration of Federal gun control laws.

In conducting these tests, we created fictitious identities and counterfeit identification documents such as driver's licenses, birth certificates, and Social Security cards. We did this using inexpensive computer software that is readily available to any purchaser.

One of the boards over there shows reproductions of some of the counterfeit identification that we created, although the photos of our agents have been deleted from the reproductions you see before you.

Our work leads us to three basic conclusions. First, government officials generally did not recognize the documents that we presented as counterfeits. Second, many government officials were not alert to the possibility of identity fraud, and some failed to follow security procedures. Third, identity verification procedures need to be improved.

Our work reveals that homeland security is vulnerable to identity fraud and, unless action is taken, individuals who intend to cause harm can easily exploit these vulnerabilities.

During each of our tests, we found that government officials did not recognize that the documents we presented were counterfeit. For example, during our driver's license investigation, we used counterfeit driver's licenses to obtain genuine driver's licenses in seven States and the District of Columbia.

Motor vehicle department employees did not recognize out-of-State driver's licenses we presented as counterfeits and issued the genuine licenses to our investigators.

During our border security investigation in which we used counterfeit driver's licenses and birth certificates to enter the United States from various western hemisphere countries, border inspectors never questioned the authenticity of the documents that our investigators presented and they had no difficulty entering the United States.

In another test, we obtained Social Security numbers for fictitious children when investigators posed as parents of newborns and submitted counterfeit birth certificates and baptismal certificates.

Additionally, we breached the security of airports and Federal office buildings, even driving a rented van into the courtyard of the Department of Justice, because no one questioned the authenticity of our counterfeit identification. These results point to the need for training of government personnel in recognizing counterfeit identification documents.

We also discovered that many government officials were not alert to the possibility of identity fraud, and some failed to follow security procedures. For example, we found that some security personnel did not look at photo identification.

As a result, officials allowed one of our agents, who presented identification containing the photo of another person, to enter a Federal building in Atlanta. Another investigator entered a Federal building and obtained a building pass and an after-hours access code from security personnel who did not follow procedures to verify his identity.

In addition, this investigator was able to obtain a building pass that identified him as a law enforcement officer and permitted him to bring a firearm into that building.

Another investigator presented a counterfeit building pass to a security officer and obtained from the officer an access code that could be used to enter the building after working hours.

Additionally, even motor vehicle department employees who recognized irregularities in the documents we presented were not alert to the possibility of identity fraud.

For example, one employee noticed that the date of birth on an investigator's counterfeit birth certificate did not match the birth date assigned to the Social Security number that he provided.

Another employee questioned the validity of an investigator's birth certificate because of the texture of the paper and because it did not contain a seal. In each instance, however, employees who saw these irregularities returned the documents to our investigators.

In at least one of the States we visited, motor vehicle department employees are required to confiscate documents they believe to be fraudulent and alert other State driver's license offices. However, the employees failed to do this.

Our work clearly points to the need for improved identity verification procedures. For example, current procedures followed by border inspectors and firearms dealers often consist of what we call a negative check. That is, a database is queried for information about the specific name that is submitted.

This process reveals whether the database contains information about the name submitted, but does not verify the identity of the license applicant or the authenticity of the license presented.

When we purchased firearms from licensed firearms dealers using counterfeit driver's licenses, the majority of firearms dealers we contacted complied with laws governing such purchases, including the need for an instant background check.

However, the instant background check only discloses whether the prospective purchaser is a person whose possession of a firearm would be unlawful. Consequently, if the prospective purchaser is using a fictitious identity, as our investigators did, an instant background check is not effective.

Our border security tests pointed to the same problem. Because immigration regulations do not require U.S. citizens traveling from countries in the western hemisphere to present a passport when entering the United States, people entering from those countries commonly present driver's licenses to the border inspectors.

However, border inspectors have only very limited means of checking with the States to verify identity or to determine whether a driver's license is authentic.

In summary, while some of the problems our tests revealed have been addressed by the responsible agencies, much remains to be done. A driver's license is the most commonly accepted document used to identify an individual.

The weaknesses we found during these investigations clearly show that border inspectors, motor vehicle departments, and firearms dealers need to have the means to verify identity and to determine whether driver's licenses presented to them are authentic.

Improved verification procedures could minimize vulnerabilities that arise when government officials do not recognize counterfeit documents or are not alert to the possibility of identity fraud.

In addition, there is a need for training of government officials who review identification in the recognition of counterfeit documents. These officials also need to be more vigilant for identification fraud.

The other chart which appears here is a brief timeline of the various tests that we performed and which I have described here today.

Mr. Chairman, that completes my statement. We will be very happy to answer any questions which you may have.

The CHAIRMAN. All right. Thank you.

[The prepared statement of Mr. Cramer appears in the appendix.]

The CHAIRMAN. Mr. Lockhart?

STATEMENT OF HON. JAMES LOCKHART, DEPUTY COMMISSIONER, SOCIAL SECURITY ADMINISTRATION, BALTIMORE, MD

Mr. LOCKHART. Mr. Chairman, thank you for asking me here today to discuss issues surrounding document fraud, identity theft, and misuse of Social Security numbers.

Although the Social Security number started just as a means to track earnings in the 1930's, it has become the single most widely used identifier for Federal and State governments, as well as the private sector.

As uses of the number have increased, especially in the private sector, so has the potential for misuse. The tragic events of September 11th brought home the need to strengthen Social Security number safeguards.

Commissioner Barnhart and I have made this a major agency priority. Social Security's key role is to ensure the integrity of what we call the numeration process, and especially the 18 million cards issued annually, and, second, to help verify Social Security numbers.

We have made a number of significant enhancements in the last 2 years and are continuing to improve these safeguards.

In the fall of 2001, Social Security formed a high-level team to strengthen our ability to prevent criminals from using Social Security numbers and cards to advance their activities.

Let me briefly review some of our efforts to date. First, we quickly began to retrain all of our employees on the rules for enumerating individuals, and we concentrated especially on non-citizens.

On July 1, 2002, we began to verify for Department of Homeland Security, or its predecessor, INS, any documents issued by them before assigning a Social Security number.

We now have an "Enumeration and Entry" process administered jointly with the Department of State, that assigns numbers and issues cards to selected non-citizens, allowing them to enter the country as permanent residents.

We have also revised our verification process for young children. Although the vast majority of children receive a Social Security number through what we call our "Enumeration at Birth" program, the parents may still apply through the local Social Security office. In June of 2002, we began verifying all birth certificates for children over age one.

Social Security is leading a new government project known as "E-Vital", to compile and verify death and birth records electronically. We opened a Social Security Card Center in Brooklyn to bring a tighter overall focus to assigning Social Security numbers.

Our employees work with those in the Inspector General and the Department of Homeland Security. The results have been very encouraging and we are considering adding additional card centers.

We have drafted a regulation to stop assigning Social Security numbers to non-citizens for the purpose of applying for driver's licenses. That reinstates a policy that was overturned by a court this year.

Turning to the subject of Social Security number verification, we currently provide over 770 million verifications a year. That is almost three verifications for every active card.

Requests continue to grow rapidly. Users include employers who verify their new hires, and a full range of government agencies, including law enforcement agencies.

It is important to remember that, when we receive a request for verification, all we can really verify is whether the information included in the request—the name, the Social Security number, and the date of birth—matches the information in our records. It is no guarantee that the person presenting that number is, in fact, the person to whom it was originally issued.

Since 1997, Social Security has worked to provide a verification service tailored specifically for the departments of motor vehicles in the States. Our online verification service enables them to request verification while processing a driver's license application. Requests are processed in one second or less for over 90 percent of the requests.

In 2004, we expect to process almost 20 million verification requests, which will more than triple this year's number. We now have 34 States signed up for this online system, of which 22 are active users.

The online system provides verification information to the DMV while the driver's license applicant is still at the counter, unlike the "batch" system referred to in the GAO report, which is only used by seven States.

Also, unlike the online system, the batch system does not provide a death indicator. We are committed to expanding the online service because we believe it is the best way to improve the integrity of the licensing system.

In conclusion, we believe that the improvements we have implemented make it much more difficult for individuals to obtain or use Social Security numbers through fraud.

I cannot over-emphasize our commitment to strengthening the integrity of the Social Security enumeration and verification processes and to work with other agencies with the goal of thwarting identity crimes that burden Americans and threaten the security of our Nation.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Mr. Lockhart.

[The prepared statement of Mr. Lockhart appears in the appendix.]

The CHAIRMAN. Now, Mr. Pistole?

STATEMENT OF JOHN S. PISTOLE, ACTING ASSISTANT DIRECTOR, COUNTERTERRORISM DIVISION, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC

Mr. PISTOLE. Thank you, Mr. Chairman.

On behalf of the FBI, I want to thank you for the opportunity to be here today to talk about identity theft and document fraud as it relates to counterterrorism issues.

Unfortunately, last week's article in a local Washington periodical was not uncommon when it spoke about three Virginia men who filed numerous fraudulent labor certificates on behalf of Korean immigrants, and then used the bogus documents to obtain green cards to remain illegally in the U.S.

One of the defendants in that investigation used a fake Social Security account number to obtain credit cards, bank accounts, and a driver's license.

The Federal Trade Commission, just last week, released a survey on identity theft and stated the problem is far worse than officials had believed. Last year, identity theft cost consumers more than $5 billion in expenses, while costing banks and other businesses over $48 billion.

As the committee is well aware, the FBI, along with a number of other Federal agencies here at the table, as long with the State and local members through the Joint Terrorism Task Forces, investigate while the Department of Justice prosecutes individuals who use those identities and document fraud to perpetrate crimes.

There are a number of Federal statutes, as the committee is aware, on bank fraud, credit card fraud, wire fraud, mail fraud, money laundering and so forth, so there are some tools there.

But, as we know, document fraud and identity fraud has been, is, and will continue to be a problem for the U.S. Government, especially when it comes to terrorism matters.

It is not a new issue to the intelligence community or law enforcement. Many folks in the hearing room may be familiar with the book and movie, "Catch Me If You Can" by Frank Avignale, who was a master forger 25, 30 years ago in the U.S. who was able to use fraudulent documents to go on a spree across the United States and overseas for several years, until he was tracked down, both as an airline pilot, impersonating a doctor, a lawyer, any number of different professions.

For decades, fugitives have changed identities to avoid capture, and check forgers have assumed the identity of others to negotiate stolen and counterfeit checks.

What is critical today is the pervasiveness of the problem and the use by terrorist of these stolen documents or fraudulent documents. The FBI does not view document fraud and identity theft as a separate and distinct crime problem.

Rather, we see identity theft and document fraud as a component of many types of crimes which we investigate along with our partners, especially in the Department of Homeland Security.

There have been a number of advances in different types of hardware and software which are in my written statement that I will submit for the record. We will not go into those at this time.

Let me just give the committee a couple of examples of some terrorist matters where document fraud has been a problem. The al Qaeda terrorist cell in Spain used stolen credit cards and fictitious sales scams for numerous other purchases for the cell.

They kept those purchases below levels where identification would be required. They also used stolen telephone credit cards for communications back to countries that supported terrorism at that time where terrorist cells were located. Extensive use of travel documents and false passports were used by that cell.

While the 9/11 hijackers did not utilize fraudulent identification, they did obtain U.S. identification cards in their names. If I could just correct the record on a statement made previously, there was only one of the hijackers, Zia Jara, who actually had a legitimate

Virginia driver's license. There were six other hijackers who had Virginia identification cards, but not a driver's license.

The hijackers were here, obviously, under terms much different than post-9/11 scrutiny. We believe that they would not be able, obviously, to operate with the impunity that they did at this time.

There have also been some domestic terrorists who have used false identity. Again, those are in my record. The one I will point out is Timothy McVeigh, obviously, responsible for the Oklahoma City Murrah Federal Building bomb on April 19, 1995. When arrested and searches conducted, Timothy McVeigh had nine aliases, different false identification.

We also have some other examples from some of the detainees from Afghanistan and elsewhere who we have interviewed. I will give a couple of examples. A Pakistani detainee who served as a doctor and a guard for the Taliban was detained at JFK Airport for attempting to enter the U.S. on a forged passport.

An Iraqi detainee purchased a false Moroccan passport for approximately $150 U.S., and used it to enter Turkey, where he was arrested. An Algerian detainee requested asylum in Canada after entering that country on a false passport. There are several other examples which are in my written testimony.

The FBI has implemented a number of initiatives to address the various fraud schemes being utilized by terrorists to fund these terrorist activities. One involves targeting fraud schemes being committed by loosely organized groups, which may then fund terrorist cells either knowing or unwittingly, simply a matter of business for them.

Many of these groups may not be, themselves, terrorists, but then the proceeds are used for terrorist activity. There are other examples listed in my written statement which I will submit for the record.

There is also an initiative which we are working with the Social Security Administration on to identify fraudulent Social Security identification cards and numbers through which we are able to assess the authenticity, and then through various means, determine whether those may be used by terrorists. Again, details are in my written statement.

I want to thank you, Mr. Chairman, for the opportunity to be here today.

The CHAIRMAN. Thank you, Mr. Pistole.

Now, Mr. O'Carroll?

STATEMENT OF PATRICK O'CARROLL, ASSISTANT INSPECTOR GENERAL FOR INVESTIGATIONS, OFFICE OF INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, BALTIMORE MARYLAND

Mr. O'CARROLL. Good morning, Chairman Grassley and Senator Lincoln. Thank you for the invitation to this important hearing.

Social Security number misuse, identity theft, and their correlation to Homeland Security has a very personal meaning to me. Two years ago on 9/11, I was in New York City and watched the Twin Towers collapse.

Since then, the SSN's role as a national identifier has solidified. You have my statement for the record. Now I would like to discuss several issues that I think are important.

First, let me discuss identity theft and the SSN. In many cases, identity theft begins with the misuse of a SSN. The SSN can be obtained in many ways: presenting false documentation to SSA; stealing another person's SSN; purchasing one on the black market; using the SSN of a deceased individual; or, creating a nine-digit number out of thin air.

The fraudulent SSN is then used in conjunction with counterfeit identity documents; such as those on display on the table in front of you, and on the video where we are demonstrating the ease in which counterfeiting visa documents can be done. This demonstration was done in a matter of minutes using seized templates, PCs, and printers.

Misused SSNs, stolen or misappropriated birth certificates, and false or fraudulently obtained driver's licenses are the keys to identity theft in the United States. We investigate thousands of SSN fraud and identity theft cases every year.

We often find the criminals have not only stolen or forged SSNs, but have stolen or forged driver's licenses as well. Because of this, we continue to work closely with law enforcement agencies and the American Association of Motor Vehicle Administrators to enhance the integrity of the driver's license.

Now I will discuss our role and that of the SSN in Homeland Security. Our Office of Investigations involvement in Homeland Security began on 9/11. Our agents assisted in the rescue efforts and site security at the World Trade Center.

Immediately after the attacks, we assigned supervisors and agents to the FBI command centers in New York City, New Jersey, and Washington, DC to process information and to investigate leads. We are members in almost 100 Joint Terrorism and Anti-Terrorism Task Forces and have participated in over 130 Department of Justice sponsored Homeland Security projects focused on the Nation's critical infrastructures, including 63 airports and 24 nuclear facilities.

These projects resulted in over 1,200 arrests. Our Office of Counsel has detailed attorneys to U.S. Attorneys' offices to assist in SSN prosecutions. Our Des Moines and our Detroit field offices were actively involved in the investigation of the earlier witness, Youssef Hmimssa.

In addition to several other charges, he was charged with, and plead guilty to, conspiracy to obtain false Social Security numbers.

According to a Syracuse University report, in the year following 9/11, nearly half of the terrorism prosecutions were initiated by SSA OIG and the now Bureau of Immigration and Customs Enforcement (BICE). We continue to work closely with BICE and other Federal, State, and local law enforcement agencies.

In addition, our Office of Audit has devoted much of its efforts to SSN integrity and Homeland Security. In fiscal year 2000, we estimated that SSA issued at least 63,000 SSNs to non-citizens based on invalid and fraudulent immigration documents.

We stressed that it is critical that SSA aggressively verify the authenticity of documents. Last year, SSA issued approximately 18

million original and replacement SSNs. The sheer magnitude of this number causes us concern over the possibility of fraud.

I am a member of SSA's Enumeration Task Force that addresses these concerns and others, including non-work SSNs and 100 percent verification of documents. These changes will deter individuals like Mr. Hmimssa from obtaining a legitimate SSN with fraudulent documents. We are also moving to establish an OIG SSN Integrity Protection Team to further combat SSN misuse and identity theft.

Mr. Chairman, in summary, all law enforcement agencies need the same SSN cross-verification capabilities currently available to employers. Legislation requiring mandatory cross-verification of identification data between governmental, financial, and commercial holders of records and SSA on a reoccurring basis is essential.

The House now has H.R. 2971, which would enhance the Social Security Act by limiting the use and display of SSNs in circulation in the public and private sector, placing restrictions on the issuance of replacement cards; and strengthening the present arsenal of criminal, civil, and administrative penalties to deter and/or punish identity thieves and those who assist them.

Identity fraud counterfeit documents and SSN misuse are growing threats to both our economic health and Homeland Security. We appreciate your interest in these issues and look forward to working with you to enhance the physical safety and financial security of all Americans.

Mr. Chairman, again, thank you for your concern and your attention, and I will be happy to answer any questions.

The CHAIRMAN. Thank you.

[The prepared statement of Mr. O'Carroll appears in the appendix.]

The CHAIRMAN. I am going to concentrate my questions in the beginning on the General Accounting Office, as well as Mr. Hutchinson, because we promised Mr. Hutchinson, who needs to leave early, that we would accommodate that.

So I am going to start out by saying that we heard that the General Accounting Office had a lot to say about different security problems that stem from document and identity fraud.

I would go to you, Mr. Malfi, with your law enforcement background. Could you put this in perspective and string these operations together for what they could mean for a terrorist group?

Mr. MALFI. Basically, if you take the operations that we conducted, string them out in order, not chronologically the way we did them but in order to show a mission, we were able to successfully sneak into the country using fictitious names and false identification on the counterfeit documents.

From those counterfeit documents, we were able to turn those and use those as breeder documents to turn them into legitimate documents, driver's licenses, to establish a true and legitimate identity within the United States.

Based on that, we were able to obtain firearms and we had access to Federal buildings. So, I guess if you draw the string out, you can see what damage could be done if these things were done in that order and for a reason that was not to test the security, but to damage it.

The CHAIRMAN. Mr. Hutchinson, I ask this question in light of the fact that we all have to be realistic. You are in a new department with a new drive to protect the homeland. But as I see it, as I think we would all agree, it is a pretty scary scenario laid out here.

Your directorate is in charge of a lot of the areas that Mr. Malfi just talked about, especially borders and airports, or maybe everything that the whole General Accounting Office report deals with. If the GAO could do all of these things, how can we be sure that your department can stop terrorists from doing it?

Mr. HUTCHINSON. Thank you, Mr. Chairman. The GAO certainly pointed up some areas of great concern. The investigation was completed prior to the stand-up of the department and bringing on the 22 agencies. But I will certainly recognize that it is a problem that is ongoing, and a concern that we have today.

I think the American public should be assured, first of all, that the steps that Secretary Ridge took in combining our inspection forces on the border will enhance our training capability and will be able to do a better job.

There are two things that I think are important for Congress and the administration to work on together. One, is a continued implementation of the U.S. visit in which we can have biometric capability for entry into our country and exit that will assure an identity and will help us to avoid this type of document fraud.

Second, I think that we have to look at the 240 different types of State driver's licenses that our inspectors are expected to be expert on. Do we need to have more restricted travel documents on which we can focus our training, we can focus our security measures on? So, those are policy changes as well as implementation that we will continue to work with Congress to carry out.

The CHAIRMAN. Well, then to follow up and to be more specific in my question to you, could you assure the committee that all these areas are all now secure, and the General Accounting Office could not penetrate those as they have demonstrated that they have in the past?

Mr. HUTCHINSON. Can I guarantee that each one of our 45,000 inspectors along the border could detect every driver's license that was presented as to whether it is a legitimate driver's license or a fraudulent driver's license? I cannot give the committee that assurance.

Obviously, we are working every day to have training to eliminate the fraud and to detect the fraud, but we are addressing it both in terms of the training, examination of policy, whether we should require more stringent requirements. We need to work with Congress on that.

Then, third, the implementation of a biometric feature. But until we address those issues in a broad fashion, document fraud will continue to be a problem for us.

The CHAIRMAN. Let me suggest to you that if you are not sure that it can be done, we will soon find out. I know that the General Accounting Office has operations under way, so we are going to find out if they can be penetrated.

Let me say to you, just as a final reminder, that I know your mission is very difficult. It is vitally important. But if the General Accounting Office can do this, obviously terrorists can do it.

Let me ask you this question, Mr. Hutchinson. I know that the issuing of driver's licenses is a function of State government, but it also is a homeland security issue, and as we have seen, a big vulnerability.

If your department can work with State and local first responders, I am sure that you could work with the Department of Motor Vehicle offices. Could you tell me if your department is working with States to shore this up, and if so, what has been done thus far?

Mr. HUTCHINSON. We are certainly encouraging more restrictive use of State driver's licenses, more security features, and we are trying to develop our capability to have more security features as these are presented at our borders. So, we are working with them. We pledge to work more aggressively with them. But simultaneously with that, we have to look at our policy issues and less reliance upon these documents.

Mr. Chairman, I understand that GAO might be out there presenting fraudulent documents. But the policy right now is that they do not even have to present a document.

If they come in and an inspector is satisfied that they are U.S. citizens by oral declaration, they can be admitted under our present policy. A driver's license, as a matter of policy, is looked at. But there is a serious examination of these overriding policies that we want to engage in as well.

The CHAIRMAN. I will ask Senator Lincoln if she has questions of Mr. Hutchinson before he goes. Then we will save the other questions for the next round.

Senator LINCOLN. Thank you, Mr. Chairman. I appreciate your focus on such an important issue.

Really, my questions have just focused on two areas. I would like to address it to all the panels and, Mr. Hutchinson, give you an opportunity to make some comments.

I think one of the biggest concerns that many of us have had, is that one of the major issues that we found wrong with our Nation's homeland security prior to 9/11 was a real lack of communication between our agencies, some of them operating with 1970's technology and the inability to really communicate in an efficient way among themselves. Thus, we have the creation of the Homeland Security Department.

I guess one of the things, in light of what we found from the GAO study or investigation, was something as simple as open and utilized lines of communication can really be a very cheap and efficient measure to stop some of the terrorists and criminals from obtaining documents in the first place.

I guess my question is, how much improvement have we seen in those lines of communication, and where have you all been really focusing your efforts in opening up those lines of communications?

And not so much as you have focused on the borders, Mr. Hutchinson, but in States like mine, what are the communications with those DMVs, what kind of training is occurring in States or being provided to States for those to train and education Federal and

State employees, I think, about ensuring that positively identified individuals are coming in. How do we train them to do that in a better way?

So, if you would like to answer those, I would be very grateful.

Mr. HUTCHINSON. Well, thank you, Senator Lincoln. Yes, that is a mandate of this department and a major goal is to increase the lines of communication. We are doing this, first of all, by developing secure communication capabilities with the governments, the homeland security directors of each State, regular communications with them.

Second, we are certainly trying to make available additional information for the trooper on I–40 as they pull over an individual so that they would have information. If they are someone under a Final Order of Removal, immigration status information, if it is relevant to the stop, and it is appropriate for NCIC registration.

We are, in addition, certainly trying to increase our communication with the private sector and our State and local outreach. Congress, particularly, gave us the State and local coordinator to work with the States on things such as motor vehicle registration and driver's license issues.

So, we are continuing to improve on those communications. There is much work to do, but much progress has been made.

Senator LINCOLN. Well, if you had to give an estimate in terms of how far along you were in improving those lines of communication, I know that in our State with a simple grant—I can talk to Mr. Hutchinson because he is a native Arkansan, and we are proud of that.

But in our State we were able to get a grant for the Sheriff's Association to really build a very, I think, state-of-the-art communication system on a web-based initiative which has hooked up all 75 of our counties, our sheriffs, along with our State troopers, our local law enforcement officers. They now can connect with about eight or nine other States to those kind of background checks and really do a good job at that.

If you had to give it a guess in terms of a percentage, how far along are we in communicating with States the availability of those kinds of projects where we could really interconnect a lot of different groups, not just law enforcement, but also some of these other areas where we could do some better background checks?

Mr. HUTCHINSON. Well, whenever you look at the Department of Homeland Security, our first responsibility was to get the communication systems united for the 22 agencies that came on board.

Then you have the examination of the various watch lists from the different departments, from the Department of State, Department of Justice, and Homeland Security. That is an aggressive initiative that we are carrying out. And then the information with the States. So, all of those are moving simultaneously along a very aggressive track.

I can cite anecdotal information as to how it has improved with our States. We have put additional information into the NCI system that is available to them. We have developed the information sharing capability in terms of what we receive at the border information and through the law enforcement alert.

Probably the greatest one is through the Joint Terrorism Task Forces of the FBI. That is really the link for the law enforcement communication and sharing of intelligence information, and I think it is working very effectively.

Senator LINCOLN. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Mr. Hutchinson. We will let you be dismissed now.

Mr. HUTCHINSON. Thank you for your courtesies, Mr. Chairman.

The CHAIRMAN. And thank you for your courtesy of rearranging your schedule to be with us.

I am going to go to Mr. Pistole. Could you talk about what the FBI is doing with the State Department of Motor Vehicles, whether it is working with them, or sometimes investigating their employees? I know there have been media reports recently about the FBI investigations of DMV offices.

Mr. PISTOLE. Yes, Mr. Chairman. Thank you. We typically work with State DMVs in a collaborative effort where they predicate information, for example, a suspect transaction or series of transactions, which leads them to believe, for example, that one of their employees may be engaged in fraudulent activity, either on behalf of a friend or for payment.

In those situations, as in the situation that you mentioned, we will then work in an undercover capacity with that Department of Motor Vehicles to investigate, and then eventually prosecute with Department of Justice, any individuals found to be engaging in that activity.

We have done that successfully, I know, in Virginia. There have been investigations in Michigan, and there have been several others that are still pending that I cannot comment on right now. But we do typically work in a collaborative effort, typically through our Joint Terrorism Task Force in that area.

The CHAIRMAN. Mr. O'Carroll, would you please tell us how your agency would coordinate with the Department of Motor Vehicles on law enforcement issues?

Mr. O'CARROLL. Yes, Mr. Chairman. We are in negotiations right now with AAMVA on getting the "no matches" from them. Currently, when the verification of the SSN is done by the State with SSA, there is nothing being done with those SSNs that do not match.

AAMVA will refer the "no match" SSNs to us. We are going to do a pilot program to see what this volume will be and what we can do in terms of a law enforcement response.

The CHAIRMAN. And Mr. Lockhart, I know that the Social Security Administration works with DMVs by providing verification services. It is my understanding that is in about half of the States.

But the General Accounting Office had testimony in July highlighting some loopholes. So my question is, what is being done about those loopholes within, or even beyond, the half of the States that do not provide it?

Mr. LOCKHART. Mr. Chairman, yes, we are working with AAMVA and the various State Department of Motor Vehicles. Unfortunately, about 29 States are still not using either of our systems, and obviously the most important thing is to get the States to start using them.

Our major system is an online verification system that we started in 1997 with the States. Right now, 22 States are using it and another 12 are signed up for it. This is online, so it is real-time. Clerks at the DMVs can go into our system and verify the name, date of birth, and Social Security number within seconds. We really think that is a very effective way to go and we want to bring it out to all the States.

We have another system, called a batch system, as they referred to in their testimony, that does not have all the capabilities of the online system. First of all, it takes 24 to 48 hours to get the information. Also, it does not track to our death file.

So, what we are trying to do is encourage the States to use the online system, but we will be looking at adding the death match capability to our batch system.

The CHAIRMAN. So you are working on people who have died, that there is a list of those people.

Mr. LOCKHART. We have that. There is a list that the State motor vehicles and anybody can buy of 70 million names of people and Social Security numbers that are dead. They have the capability to get it separately. But in the batch system, it is not there. But the important thing is, in the online system, that capability is there and, again, it is available real-time.

The CHAIRMAN. Yes.

And Mr. Cramer, what has the General Accounting Office then found about information sharing and verification between Department of Motor Vehicles and the Social Security Administration? Are these agencies using negative checks and positive checks?

Mr. CRAMER. For the most part, the identification/verification procedures are negative checks. By that, I mean a name or other identifying information is put into the database. If that database has information about that name or other identifying information, then it will provide that to the inquirer.

The problem, though, is if, for example, as our investigators did, if you are using a fictitious identity and there is no information in that database about your fictitious identity, then the verification will not be effective.

This happened with the gun dealers, for example. They go onto the database, which tells the names of those people who cannot buy guns, it would be unlawful. But our investigators had fictitious identities and their names were popped in, and of course nothing came back. So, it does not work. That kind of problem exists in many of these verification procedures.

Mr. LOCKHART. Mr. Chairman, I would like to point out with the online verification system, to get a match the DMV has to submit the name, Social Security number and the date of birth. So, it is a positive identification match.

The CHAIRMAN. All right.

Mr. Pistole, I would like to ask you about the number of terrorism cases that the FBI has been working on since the attack of 9/11. Could you tell me how many FBI terrorism investigations have led to terrorism charges and how many of those have led to either conviction by jury, plea bargains, or acquittal?

Mr. PISTOLE. Mr. Chairman, I will have to estimate. I was not anticipating that question, so let me just try to estimate here.

In terms of convictions, there have been at least 20 individuals who have been convicted of terrorism-related charges since 9/11 in the U.S. through the Department of Justice. Many more than that have been charged and are awaiting, either trial, or plea agreements.

For example, in Northern Virginia here, there is a group of 11 that have been indicted, some of whom have entered guilty pleas, some of whom there will be either superseding indictments brought against, or additional persons charged.

But we have had, as the committee is aware, individuals, the Lackawanna six in Buffalo, there have been individuals in Portland, Detroit, and other areas around the country who have already been found guilty.

In terms of the number of investigations, I was not clear whether you were asking how many we have pending now, or were you simply focusing on the number of convictions and people charged?

The CHAIRMAN. Well, one of the things I would like to have you respond to is whether or not there have been any other FBI terrorism cases that have led to jury convictions besides the Detroit case.

Mr. PISTOLE. I do not believe so. I believe all the other convictions have been by guilty plea. I will check on that to be sure.

The CHAIRMAN. All right. And correct it if it needs correcting.

Mr. Cramer, based on what you have heard the prisoner testify about before, does anything he said about making false documents surprise you or is this what you expected?

Mr. CRAMER. It is pretty much what I expected, Senator. Nothing really surprises us at this point. The only thing that continues to surprise us, is that it really is so easy to do this. One of the problems that we have not addressed, I know the Social Security system does do a positive check.

In one sense, if I steal someone's identity, I have their true name, Social Security number, and date of birth and I create a counterfeit document with that information, then I can use that, bring it into a motor vehicle department that does check with Social Security and it will pass. It will be fine, because that is a true person. It is not me. Now I have an identification, a true identification document issued in someone else's name. So, that is just another piece of this.

The CHAIRMAN. Mr. O'Carroll, I thought your presentation about fraudulent visas was very good, and it was probably almost too good. But what can a law enforcement agency like yours and the FBI do to stop people like Hmimssa from making these documents? I would also ask Mr. Pistole, when he is done, to answer on the same subject, and then that is my last question.

Mr. O'CARROLL. Mr. Chairman, one of the things that we feel would be the best way to prevent this would be cross-verification. We are currently doing 100 percent verification with BICE. If anybody uses a visa, we are checking the underlying documents and also verifying the information on the documents with another agency. That way, we will be able to determine whether or not the visa was counterfeit.

We feel that by this comparison of information on the visa and the sharing of information between law enforcement agencies, we

should have a much better chance of being able to verify the underlying documents and prevent the counterfeiting of them.

The CHAIRMAN. How about you, Mr. Pistole?

Mr. PISTOLE. Yes, Mr. Chairman. I would agree with what Mr. O'Carroll stated, in addition to, I think, the two-prong approach of improvements in technology to get away from a documents-driven verification system and get into biometrics and different aspects there, coupled with the information sharing from the law enforcement and intelligence community's perspective domestically through the Joint Terrorism Task Forces.

I think, as this committee is aware, we have created a National Joint Terrorism Task force with 32 Federal agencies and State agencies on it here in DC. We have 66 Joint Terrorism Task Forces around the country, with another 26 being created.

It is through that sharing of information that I think we stand the best chance of succeeding in this war on terrorism.

The CHAIRMAN. Senator Lincoln, do you have any questions?

Senator LINCOLN. Mr. Chairman, just two, briefly, if I could.

You spoke about cross-verification, Mr. O'Carroll. I am curious. I guess, Mr. Chairman, if I may ask for unanimous consent to include my opening statement in the record, as well as any questions. Particularly, there was one left for Mr. Hutchinson that I did not get to ask, which is basically on that issue of cross-verification.

The CHAIRMAN. Without objection.

[The prepared statement and questions of Senator Lincoln appear in the appendix.]

Senator LINCOLN. In terms of improving the communication among agencies, cross-verification can make a difference. We were trying to communicate among different agencies.

Is the communication that we are building, hopefully in a more state-of-the-art and up-to-date mode among these different agencies something that is going to be able to cross-reference?

I know that one of the biggest problems we found in dealing with building our research piece for our Sheriff's Association was, unless it was web-based and unless we were able to use the same modes of communication—I am not a computer specialist, but to best understand it, the same computer language—we were not going to be able to share that information with other States.

So, as we began to build what we were doing, we had to change the whole level of our system of management computer-wise in terms of the information we were storing in order to be able to interconnect with other States, because as criminals crossed our borders, we wanted to know and be able to assist other law enforcement officers and agencies in other States.

Now that we are on a web-based system, we can now interconnect with nine other States. Hopefully, that system is growing so that we can connect. But in this cross-verification, these agencies, are we all building these new systems in a way that they are going to be able to inter-communicate?

Mr. O'CARROLL. Senator, the specific computer systems that are used by the States and agencies is not my area of expertise.

I can say, on a Federal level, from agency to agency, we are having a difficult time comparing information. There are so many dif-

ferent systems, so many different sets of records. It is a Herculean task even on the Federal level.

We are recommending, just as you mentioned, bringing it down to the State level, and even bringing it into the financial community, to start taking a look at the bank records and the information individuals are providing when they are opening up bank accounts.

I think you have recognized the problem. It is going to be a long, hard road to be able to come up with interconnecting information sources to go back and forth. But we have to start down that road now or else we will never be able to solve it.

Senator LINCOLN. Well, I certainly hope that out of this hearing and the work that we can do in conjunction with the agencies, from our standpoint, is to encourage as we do improve and modernize agencies with better communications, that we think far enough into the future that we provide them with an ability, or certainly the levels of communication that are going to work among agencies, across State lines, across State and Federal lines, and other things like that. Because without that ability, any kind of improvements we make are still going to keep us back in the Dark Ages. So, I will certainly include that in my request to Mr. Hutchinson for his responses as well.

The other question I had to you, Mr. O'Carroll, is really, what training and education is being done from your standpoint, Federal and State employees, about ensuring that they positively identify those seeking original documents? Are you reaching out into the States and working with some of these people on the local level, training?

Mr. O'CARROLL. Senator, at the moment, we have not gotten to the State level. We are currently training and educating Social Security employees. We have been meeting with the State Department and with different Homeland Security organizations. We have also been dealing very heavily with the former INS, which is now BICE.

We have training sessions on document recognition for all of our agents, and we have been rolling that out, with the cooperation of Social Security, to each of the Social Security district offices and trying to train all SSA employees on how to recognize counterfeit documents.

But, unfortunately, what we are finding out, and as you can see from the documents we have as evidence in front of us, in many cases the counterfeit passport or counterfeit document looks better than the genuine. With the technology out there today, it is almost an impossible task to certify what documents are genuine or counterfeit.

Mr. LOCKHART. Senator Lincoln, from a Social Security standpoint, yes, we are working with our Inspector General to train our employees on document verification. But I think the critical thing is, now we are actually verifying them with the Department of Homeland Security, that we are not relying on our employees to look at a document and tell if it is genuine or not.

We access their computer system and we can check online whether the document has been issued by the Department of Homeland Security. If it has not, we actually then send a copy of the document to the DHS to get them to verify it.

Senator LINCOLN. Were none of these documents of the nature that they would have gone through that process?

Mr. LOCKHART. Visas would go through the process. The visa story we heard earlier today happened before we put in this process, which is about a year old.

Mr. O'CARROLL. One final point to add to what Mr. Lockhart said. We are also verifying birth certificates. That is another major breeder document that is often counterfeited. We are going back to the States of record to verify that the birth certificate is legitimate, which is a big step in the right direction.

Senator LINCOLN. Is there anything that any of you gentlemen can add to what has already been talked about, which is we know it is easier to do a negative check on an individual than a positive?

Is there anything that you think stands out of where we are doing more in the form of a positive check to positively determine that an individual is who they say they are, or any recommendations on how we improve on those positive checks? Yes, sir?

Mr. COONEY. Senator Lincoln, in the case of the driver's licenses, every DMV that we went into, not one of the employees could identify the breeder license that we were using as being counterfeit.

We think that a simple fix would be to allow them to make a positive ID check by having access to the States, the different States, that they could verify that the license presented to them is an authentic license.

Senator LINCOLN. That is a great suggestion. But, once again, in order to be able to do that, the States are going to have to have systems that will contact or communicate with one another.

So, I would just encourage all of us as we are looking forward that those means of communication are going to be necessary. They are going to have to link. But that is a great suggestion.

Thank you, Mr. Chairman, for this hearing. Very informative.

The CHAIRMAN. Thank you.

I am going to submit further questions for response in writing, and maybe you will get questions from other members who could not be here, or who were here.

But I want to thank you all very much for coming. This has been a very alarming set of testimony we have had. I think it shows that we are still too vulnerable to document and identity fraud, which then in turn means that we are still vulnerable to terrorism. I think we have had some good news of how you are mobilizing to address it. There is a lot of follow-up here. I thank you again. You are excused.

[The questions appear in the appendix.]

The CHAIRMAN. I would call the third panel to get the perspective of State involvement with this. Ms. Linda Lewis is president and CEO of the American Association of Motor Vehicle Administrators. We will have her testimony about what her organization is doing to secure the driver's license process.

Then we have Robert Douglas, CEO of American Privacy Consultants. Mr. Douglas will give us insights as an identity theft expert consultant for law enforcement and financial companies.

Also, for many years he was a private investigator here in Washington. It is my understanding he will tell us some interesting demonstrations to show how false documents are readily made.

I am going to start with Ms. Lewis. Thank you for being patient through a long hearing, probably longer than I anticipated. But it is very important.

STATEMENT OF LINDA LEWIS, PRESIDENT AND CHIEF EXECUTIVE OFFICER, AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS, ARLINGTON, VIRGINIA

Ms. LEWIS. Thank you, Mr. Chairman. Good morning. Good morning to you, Senator Lincoln.

I am Linda Lewis, president and CEO of the American Association of Motor Vehicle Administrators, or AAMVA.

AAMVA represents motor vehicle and law enforcement officials who are responsible for administering the laws governing motor vehicle operation, driver credentialing, and highway safety enforcement.

We are not surprised by the findings of the GAO investigation. In fact, we believe this investigation is long overdue. The report adds to the mounting evidence that we need to fix our driver licensing process. Many of our members are taking steps to improve the licensing process within their own State borders.

However, until we implement uniform practices, the process remains fragmented and vulnerable. As a result, we increase the opportunities for identity theft and fraud and put at risk our Nation's national security and highway safety.

AAMVA came together with numerous industry experts to develop a comprehensive solution to enhancing the licensing process. Note that I say "comprehensive." Fixing one aspect of the problem will not make a difference.

This comprehensive approach addresses tightened application requirements for obtaining a driver's license: electronic verification of an applicant's driver history and breeder documents; improved processes and procedures for issuance, including internal audits and training for employees; increased penalties for those who commit fraud; and, to ensure compliance with these activities, participation by all States in the Driver License Agreement, a new interstate compact.

Let us look at the vulnerabilities in driver's licensing and, more importantly, the steps needed to tighten the system. Currently, individuals can apply for and obtain a license in more than one State. To remedy this, we need to establish an information system that ensures each driver has only one license and one driver record.

The Commercial Driver's License Information System, which kept over 800,000 unqualified truck drivers off the road within a 4-year period, demonstrates the success of this approach.

In addition, the use of false breeder documents runs rampant within the application process. This means we must adopt a uniform resource list of acceptable identification documents, which narrows the numerous resources relied on for issuing a license.

We must provide adequate training to DMV employees. They need the tools to recognize and appropriately handle fraudulent documents, and we must ensure motor vehicle agencies have the ability to electronically verify the validity of breeder documents with the SSA, the Bureau of Citizenship and Immigration Services,

the State Department, vital records agencies, as well as other DMVs.

We also have a serious problem with fake driver's licenses and ID cards. That is because the driver's license is easily counterfeited. Today, as you have heard earlier, there are more than 240 valid license formats, all lacking uniform security features, making it easy for criminals to alter a real document or create a counterfeit license. To combat this problem, we need to adopt minimum uniform card design and security features for the license and then train others to identify fraudulent documents.

The last problem relates to human behavior. Unfortunately, some individuals break the law. America wants criminal behavior stopped on both sides of the counter.

AAMVA has recently developed model internal controls and auditing procedures for States to help detect this behavior and prevent it from spreading further.

And, most importantly, Federal and State policymakers must partner with law enforcement and the courts to implement and enforce stiffer penalties for those who choose to break the law.

For the last 2 years, AAMVA has addressed these problems with Congress. The evidence is clear. It is time we stop talking about the problem and focus on solutions, a solution that must be implemented as a comprehensive package and not a piecemeal fix, a solution that reduces identity theft and fraud, and enhances homeland security and highway safety, a solution that can protect an individual's personal privacy through adherence of privacy laws, and a solution that can only be achieved with a State/Federal partnership that includes funding and the political will.

Without a State/Federal partnership to implement these changes, this comprehensive approach is little more than a best practice.

In closing, AAMVA is not a regulatory body. We are the technical experts and we believe we have done our job by developing a comprehensive solution to this longstanding problem.

In April of 2002, we conducted a public opinion poll. The poll reveals the American public overwhelmingly favors cooperative State and Federal efforts to close one of the biggest loopholes in the United States' national security system by strengthening motor vehicle agency licensing practices. Mr. Chairman, Senator Lincoln, will you help us? Thank you.

The CHAIRMAN. Thank you. I hope that is what this hearing is partly about.

[The prepared statement of Ms. Lewis appears in the appendix.]

The CHAIRMAN. Now, to Mr. Douglas.

STATEMENT OF ROBERT DOUGLAS, CHIEF EXECUTIVE OFFICER, AMERICAN PRIVACY CONSULTANTS, OAK CREEK, COLORADO

Mr. DOUGLAS. Good afternoon, Mr. Chairman. Good afternoon, Senator Lincoln.

The now documented fact that a terrorist could potentially walk into a DMV licensing office and present obviously fraudulent documents in exchange for a driver's license, thereby increasing the probability of boarding an aircraft, just as the September 11th terrorists did, shocks the conscience.

But the extent of the problem does not end there. The same fraudulently obtained driver's license could assist terrorists and other criminals to gain access to secure facilities in order to perform a myriad of criminal activities.

Additionally, the same fraudulently obtained driver's license could assist a terrorist or other criminals to open a financial services account, transfer funds in or out of the country, launder money, or steal the funds of a legitimate account holder.

No exceptional means or methods were used by the OSI agents to deceive DMV officials. To the contrary, the fraudulent documents were prepared using equipment and software available to any individual in the world.

In the final analysis, the fraudulent documents used by the GAO undercover agents were of lesser quality than a terrorist or identity criminal could, and would, be expected to use.

The fact that a number of DMV officials did not even question the fraudulent documents presented by the agents is inexcusable, but sadly not unexpected. Prior GAO investigations and subsequent Congressional hearings have revealed that in far too many aspects we are a country lax in security.

By way of comparison, my own experience and training in auditing bank employees and identification authentication systems teaches that far too many financial services companies, called by President Bush the Nation's first line of defense in stopping the movement of terrorist funding, are woefully inadequate in their ability to provide that very defense.

There are several significant reasons for this failure: the lack of standardized identification authentication equipment and systems; the lack of appropriate security protocols within institutions; the lack of adequate training of existing protocols; and the poor performance by individual employees in following security protocols that have been provided and trained.

Mr. Chairman, it would not be a surprise that DMV officials could be deceived with high-quality fraudulent documents. It is of great concern that obviously fraudulent documents of relatively poor quality were, in a number of the tests, accepted without question.

Further, the apparent lack of standardization in reviewing the fraudulent documents and the lack of reporting or seizure of detected fraudulent documents is a glaring deficiency that must be addressed.

Let me speak a few words about the broader issue of identity theft. Just this past week, the FTC released a new survey showing that upwards of 27 million Americans have been victimized by identity theft in the last five years alone. According to the study, 10 million were victims in the past year.

The FTC's report also paints a grim picture of financial losses due to identity theft. Forty-eight billion dollars to the financial services industry, $5 billion in losses to the individual American, should ring out across America as loud as the loudest bank hold-up alarm, for that is precisely what this is, a national bank robbery under way right before our eyes.

The obvious question is, what is feeding the ease with which identity theft and identity fraud crimes are carried out? The an-

swer is multifaceted, but straightforward. First, ease of access to biographical information of all Americans. Second, lack of standardization in identity documents and authentication protocols. Third, ineffective authentication protocols and training.

The first issue. As was crudely demonstrated by a California special interest group several weeks ago outside the White House, information about all Americans is easily obtained for free or for a small fee.

The group demonstrated that they were able to purchase the Social Security numbers of the Director of Central Intelligence and the Attorney General, amongst others.

If the highest public officials of our country can have their Social Security numbers sold on the web like Elvis memorabilia on E-bay, what chance does everyone else stand in protecting their identity? After all, the Social Security number is the key that opens the kingdom for identity thieves.

The reality is much worse than that, though, Mr. Chairman. The reality is, anyone can buy anything about anybody in America today, including Social Security number, dates of birth, home and work addresses, phone numbers, mother's maiden name, DMV information, voter identification information, bank account numbers, bank account balances, investment portfolios, medical records, and the list goes on and on. That is just a partial list of what is available.

I have appended to my testimony as Appendices A and B my two previous Congressional testimonies documenting in great detail the extent of the illegal information market in America.

But for the sake of illustration, I have on the projection screens today a web site that I would like to call the attention of the committee to called hackershomepage.com. It is up this very minute as we speak all around the world.

If you go to Section 6 of the web site, it is actually selling portable magnetic stripe card readers and writers.

All of the equipment, if you look through this section, Mr. Chairman, to set up your own identity theft operation, precisely the equipment that I noticed Mr. Hmimssa testified to this morning in his written testimony, or the written declaration of his testimony, that he used to skim information off of credit cards in his taxi cab, put it on his credit card, build up his bank account, and build up his ability to stay in this country.

That is not the only type of web site. There are hundreds, Mr. Chairman, of web sites out there selling every piece of information about all of us.

I would also like to talk about the lack of standardization. In the U.S., we have a dizzying array of forms of officially distributed State DMV driver's licenses and forms of underlying documents accepted by DMVs for issuance of the licenses. It is reported that there are currently 400 official formats of State-issued driver's licenses and non-driver IDs.

So, we have hundreds of officially issued State identifications that no one in the United States, including any of the gentlemen on the panel before us, can conceivably determine the validity thereof with any degree of certainty. Yet, that is precisely what

stands between the next Mohammed Atta and access to a U.S.-based airliner today.

Compounding the problem presented by the variation in current State-issued identification documents is the equally dizzying variation in underlying documentation accepted for the issuance of a State license.

These documents include Social Security cards, birth certificates, foreign and domestic passports, green cards, and foreign matricula consular cards.

As if that were not enough, add the fact that there are no consistently available reliable or secure methods for determining the authenticity of any of the documents described so far.

The bottom line, Mr. Chairman. It really is quite simple. In the United States today, we have a State-issued identification system predicated upon a fiction built upon a fallacy.

The fiction is the belief that current State-issued identification systems afford us a level of security. The fallacy is the belief that State-issuing officials can, and will with certainty, issue license or identification cards to only the individual named on the license or ID card.

In conclusion, looking at ineffective identification protocols, the worrisome fact that a number of State officials did not recognize the presented documents were fraudulent demonstrates the lack of appropriate authentication protocols, the lack of available authentication systems, and the lack of training to available systems and protocols, or perhaps all three depending upon the individual State.

The most worrisome factor of all, is that a number of officials did recognize the documents as fraudulent, but proceeded to allow the undercover agent to leave with the fraudulent documents absent any apparent notification of appropriate law enforcement, or even supervisory officials.

I have seen this problem on an almost universal basis during my work with the private sector. For much of corporate and governmental America, customer service comes before a sense of security. That was acceptable before 9/11. It is not today.

Security must stop being an afterthought that is viewed by corporate America and government agencies as an albatross that either does not contribute to the bottom line, or takes away too many dollars from other governmental programs.

To this day, there are hundreds upon hundreds of banks in America that an identity thief, armed with the biographical data of a legitimate bank account holder, can steal money out of an account by phone simply because the bank refuses to change the authentication protocol from a biographical fact that any thief can purchase on an Internet to a PIN only known by the account holder. This is not theory. It has happened time and time again, with very prominent Americans being the victims of bank robbery by phone. It may be the easiest crime in America today.

The problem, as demonstrated by the GAO report released today, is not confined to the financial services industry. It is an American problem. It pervades every private and public sector.

It is a problem of attitude and determination, having the attitude to accept the need for effective authentication protocols, combined

with the determination to see the protocols trained and followed to the degree needed for effectiveness.

Thankfully, we have historically had a country where security did not need to be paramount in our thinking and daily business and government practices. Unfortunately, as demonstrated by 9/11, the recent FTC survey, and many other daily examples and reminders, those carefree days are gone.

I stand ready to answer the questions of the committee.

The CHAIRMAN. Thank you very much.

[The prepared statement of Mr. Douglas appears in the appendix.]

The CHAIRMAN. Ms. Lewis, could you tell us what Federal agencies you work with and the extent of that work that you do with them? I would be especially interested in any interaction you have with the Department of Homeland Security.

Ms. LEWIS. Well, we are just beginning that cooperation there. There are several agencies that we have worked with, the Social Security Administration, the Department of Justice, the Department of Transportation and agencies there, FMCSA, the National Highway Traffic Safety Administration, the FBI, the Secret Service, the Canadian Mounted Police are also involved, and other associations, the IACP.

Homeland Security is a new partner for AAMVA, closely with the TSA, particularly with regard to the Patriot Act and implementation of that law.

So, we are beginning the dialogue with homeland security and are looking forward to collaborating even more. As a matter of fact, I just left a message with Asa Hutchinson as he left here that we, indeed, need to sit down and discuss collaboration.

The CHAIRMAN. And with most of the agencies that you have made contact with, and obviously talking about what you consider mutual problems between States and the Federal Government, have you found the cooperation like you would expect it to be under the circumstances of the war on terrorism and the concern about terrorism, and obviously fake documents? Or do you think that there is something the Federal Government should be more responsive to with entities like yours?

Ms. LEWIS. I think we would hope there would be more responsiveness. We have been on this podium, probably, ever since 9/11. We really did spend a year, probably a year and a half, defending our position against those who thought we were trying to do more than just correct a driver's licensing process that is broken today.

We have wasted a year and a half and we did not have the support for the political will of Congress, nor the State legislatures at that time. I am pleased to say that that is changing.

The fact that I am sitting here before you today says that that is changing. The fact that we have had government officials all talking about a problem that has basis with the application and the processing of the driver's license, as well as other ID documents, it tells me that we have made progress. There is still more to be done in a partnership fashion, not just the States, but in collaboration with the Federal Government.

The CHAIRMAN. Well, considering the issues that have been laid out here today and the awakening that this hearing ought to pro-

vide everybody, I can only speak for myself, but the extent to which I or my staff can help in being a conduit between your organization and any Federal agency, please let me know.

Ms. LEWIS. Thank you.

The CHAIRMAN. I have one last question, and that would be to both of you. I know that there are legislative proposals. But is there anything that Federal agencies can do on their own initiative right now to make driver's licenses more secure, even though States are in charge of that?

Ms. LEWIS. I would like to go first, if I may. I think there are a lot of things you can do. One, is to recognize that there is a problem. I think many of us have had our heads in the sand that the problem even exists.

I really do applaud the committee and Congress for conducting this GAO investigation, because I think it does provide credible evidence that, in fact, a problem does exist.

I think that is the first thing, the political will, asking the States, talking to the Governors of your States and the State legislatures to take this issue seriously.

I think the development of some type of a grant program, an incentive program for the States to encourage them to do those things that go a long way to improve the system might be another step in the right direction as well.

Mr. DOUGLAS. I would echo much of what Ms. Lewis has said. As an outside observer, I know their organization has been, for a number of years, trying to address some of these problems. I think the political will does need to come from Congress.

Any time that you start talking about what I think is very apparent from listening to this whole hearing today, that the only solution is going to be standardization, reduction of the number of documents that are currently being accepted, whether it is for entry into the country, whether it is for acceptance by any of the different 50 States, for the issuance of driver's licenses, when you start talking about putting security features into driver's licenses and into the other breeder documents, of course, the hue and cry comes up about a national ID card, that we are federalizing a system and all of the political concerns therein.

The reality is, all of these systems are out there. All of the information about all of us is either in government hands, or I could demonstrate ad infinitum that it is already in the private sector.

As I said before, you can buy anything about anybody in this country on the Internet right now. The only one who seems to be behind the eight ball is the government in the ability to know, when I present a driver's license, is that, indeed, Rob Douglas on the driver's license? The reality is, no one in this country can do it. It is a totally fallacious system that we have for security right now.

When we present our driver's license at the airport, it means absolutely nothing currently. I looked at my driver's license while I was sitting here waiting to testify. There is some bar coding on the back of it. I have had that license for years, and no one has ever used that bar coding for anything in the country.

So I think, as Ms. Lewis says, we recognize the problem is here. That recognition has been growing with the ongoing serious of

GAO investigations, culminating today. And I love the chart that they had over there documenting almost precisely how a terrorist could enter this country, become one of us, and carry out an act.

With the hearing today, I think the culmination of all that can go wrong is here, we just need to bring all the parties together and there needs to be standardization of these documents, otherwise they mean absolutely nothing and we are just wasting money.

The CHAIRMAN. Well, that is the last question I have. You may get questions from other people for answer in writing. I would appreciate your response to those about 2 weeks after you have received them.

I want to say that I consider your testimony very worthwhile. Both of you are very forceful in what we need to be doing. Hopefully, we can help each of you along in your drive, because it is mutually beneficial to us.

We have heard today about the legitimacy of the problem and the illusion that there is legitimacy to people that claim to be something that they are not, and the threat that that is to national security. Hopefully, this hearing will help focus attention on it and will move along more quickly.

With that, I thank all of you, and the hearing is adjourned.

Mr. DOUGLAS. Thank you, Mr. Chairman.

Ms. LEWIS. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

[Whereupon, at 12:58 p.m. the hearing was concluded.]

APPENDIX

Committee On Finance

Max Baucus, Ranking Member

NEWS RELEASE **http://finance.senate.gov**

For Immediate Release
Tuesday, September 9, 2003

Contact: Laura Hayes
202-224-4515

STATEMENT OF SENATOR MAX BAUCUS
DRIVER'S LICENSE FRAUD OVERSIGHT HEARING

Thank you Mr. Chairman for convening this important hearing as our country nears the second anniversary of the September 11th terrorist attacks.

In January, President Bush spoke to the nation and reminded us how high the stakes ride in our nation's efforts to fight the war on terror. In reference to the war on terrorism, he said "as we fight this war, we will remember where it began: in our own country." He said, "we've intensified security at the border and ports of entry." After the President's speech, this Committee held a hearing to assess the security of our borders. In that hearing, serious questions were raised about whether the government was doing enough.

Today's hearing focuses on another critical aspect of how we protect our homeland -- the adequacy of systems used to issue identifications to people in our country. Specifically, we will focus on the apparent ease with which an authentic driver's license can be obtained by using fictitious documents.

This Committee exercises jurisdiction of identity fraud through its oversight of the use of Social Security numbers. Social Security numbers play a vital role in verifying identity. And, while the Social Security Administration has taken some steps to prevent the misuse of Social Security numbers, problems still persist. Today, we will hear about two recently-discovered gaps in the protection of these numbers. I also want to hear what SSA is doing to close these gaps.

But, why is the issue of identification fraud important? It is worth remembering that seven out of the 19 September 11th hijackers fraudulently obtained authentic driver's licenses through the Virginia Department of Motor Vehicles. They used these authentic driver's licenses to board the planes on that tragic day.

Even today, there are press reports that Virginia DMV workers were part of a lucrative scam that trafficked in bogus Virginia driver's licenses – and netted more than $1 million. Last month, a man from Guinea was charged with using a false Social Security number to cash counterfeit checks as part of another conspiracy that obtained over $1.2 million. The suspect admitted having three Virginia driver's licenses. For one, he told DMV workers he changed his name for religious reasons. For the second license, he used an international driver's license. And for the third license, the DMV allowed a friend to vouch for his residency. It remains clear that a weak link in our national security chain still exists.

A driver's license is a commonly acceptable form of identification. It also plays an integral role in helping to protect our national security. Not only are licenses used to board airplanes, they make it possible to re-enter the United States, obtain access to government buildings, open bank accounts, cash checks and buy weapons. What is most important about a driver's license is the apparent legitimacy it establishes.

Driver's licenses – like all government-issued IDs -- carry a presumption of authenticity. When we see these forms of ID, we presume the persons possessing them are who they say they are. We lessen our suspicions and drop our guard. We assume the government has done its job in checking out the person's credentials and has validated the person's true identity. Unfortunately, as we will hear today, this is not always the case.

GAO will tell us today that -- two years after 9/11 -- many DMVs remain susceptible to fraud and abuse. The GAO will testify that DMVs are not alert to the possibility of identity fraud. Some workers at the DMV failed to follow security procedures and report attempts to create false identities. In other cases, DMV workers told the GAO investigators what they needed to do to fix their fraudulent documents.

We will also learn that DMV offices do not have access to the appropriate information systems to fully carry out the background checks they need to perform. In a time of heightened national security, state DMVs play an integral role in protecting us. A driver's license is more than a license to drive. It is the primary document we use to identify ourselves. Accordingly, DMVs have a responsibility to look beyond driving safety and detect counterfeit documents used to establish identity. Frankly, the DMV vulnerabilities are inexcusable.

So, what are we going to do about the problem? Today, I would like to offer some solutions to these problems. First, we need better standards for issuing identity documents. This will increase detection of fictitious or fraudulent documents used to establish identity. Next, we need to ensure that DMV workers are better trained to identify counterfeit documents. Third, we need more sophisticated technology at the DMVs. The Department of Homeland Security was created to facilitate communication among agencies. We also need to ensure that DMVs can communicate with each other and with law enforcement officials. And last of all, DMV workers need to become more vigilant to prevent bad actors from obtaining valid driver's licenses.

Mr. Chairman, today's hearing is very timely – and disturbing. I look forward to hearing from the witnesses. I am particularly interested in learning what specific steps the Administration is taking to address the security weaknesses identified by our witnesses. Talk is cheap. The American people deserve and expect action. Thank you, Mr. Chairman.

United States General Accounting Office

GAO

Testimony
Before the Senate Committee on Finance

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, September 9, 2003

SECURITY

Counterfeit Identification and Identification Fraud Raise Security Concerns

Statement of Robert J. Cramer, Managing Director
Office of Special Investigations

GAO-03-1147T

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you today to summarize some of our recent investigations that demonstrate security vulnerabilities that exist because counterfeit identification can be easily produced and used to create fraudulent identities.

My testimony today is based in part on the recently issued restricted report *Security: Vulnerabilities Found in Driver's License Applications Process.*[1] My remarks also encompass results from security tests we have performed over the past 3 years. These tests revealed security weaknesses at federal buildings and other facilities, airports and our nation's borders, and exposed identity fraud vulnerabilities in both the Social Security number (SSN) application process and in the administration of federal gun control laws. (See app. I for a synopsis of the tests we have conducted since 2000.) A number of these problems have been addressed by the responsible agencies.

In conducting these tests, we created fictitious identities and counterfeit identification documents, such as driver's licenses, birth certificates, and Social Security cards. We did this using inexpensive software and hardware that are readily available to any purchaser.

In summary, we found that (1) government officials generally did not recognize the documents we presented as counterfeits, (2) some government officials failed to follow security procedures and were not alert to the possibility of identity fraud, and (3) identity verification procedures are inadequate. Our investigations revealed that homeland security is vulnerable to identity fraud and, unless action is taken, individuals who intend to cause harm can easily exploit these vulnerabilities. Additionally, identify fraud has a range of other consequences including potential fraud in voting, obtaining credit and federal benefits, and in many other areas.

[1] U.S. General Accounting Office, *Security: Vulnerabilities Found in Driver's License Applications Process*, GAO-03-989RNI (Washington, D.C.: Sept. 9, 2003).

Government Officials Did Not Recognize Our Counterfeit Documents

During each of our tests, we found that government officials did not recognize that the documents we presented were counterfeit. For example, during our driver's license investigation, we used counterfeit driver's licenses to obtain genuine driver's licenses in seven states and the District of Columbia. Because motor vehicle department employees did not recognize as counterfeit the documents we presented, including out-of-state driver's licenses, they issued genuine licenses to our investigators. During our border security investigation, in which we used counterfeit driver's licenses and birth certificates to enter the United States, border inspectors never questioned the authenticity of the documents and our investigators encountered no difficulty entering the country. In another test, we obtained SSNs for fictitious children when investigators posed as parents of newborns and submitted counterfeit birth certificates and baptismal certificates. Additionally, we breached the security of airports and federal office buildings because no one questioned the authenticity of our counterfeit identification. Additional training of government personnel in the detection of counterfeit identification documents is sorely needed.

Some Government Officials Failed to Follow Security Procedures and Were Not Alert to the Possibility of Identity Fraud

We also discovered that some officials failed to follow security procedures and were not alert to the possibility of identity fraud. For example, we found that some security personnel did not look at photo identification. As a result, officials allowed one of our agents, who presented identification containing another person's photograph, to enter a federal building in Atlanta. Another investigator entered a federal building and obtained a building pass and an after hours access code from security personnel who did not follow procedures to verify his identity. In addition, this investigator was able to obtain a second feature added to the building pass that identified him as a law enforcement officer and permitted him to carry a firearm. Yet another investigator presented a counterfeit building pass to a security officer and obtained from the officer an access code used to enter the building after working hours.

Additionally, even motor vehicle department employees who recognized irregularities in the documents we submitted were not alert to the possibility of identity fraud. For example, one employee noticed that the birth date on an investigator's counterfeit birth certificate and other records did not match the birth date assigned to his SSN. Another employee questioned the validity of an investigator's birth certificate because of the texture of the paper and because it did not contain a seal. In each instance, however, employees who saw such irregularities returned

the documents to the investigators. In at least one of the states we visited, Department of Motor Vehicle (DMV) employees are required to confiscate documents that they suspect to be fraudulent and send a teletype alerting all state driver's license offices of the facts surrounding the questionable documentation. However, this policy was not followed.

Improved Verification Procedures Are Needed

Current verification procedures followed by border inspectors and firearms dealers often consist of what we call a "negative" check; that is, a database is queried for information about the specific name or other personal identifiers submitted. This process reveals whether the database contains information about the name submitted but does not verify the identity of the license applicant or the authenticity of the license presented. For example, we purchased firearms from licensed firearms dealers using counterfeit driver's licenses. The majority of firearms dealers we contacted complied with the then-existing federal and state law governing such purchases, including instant background checks required by the Brady Handgun Violence Prevention Act of 1993.[2] However, the instant background check only discloses whether the prospective purchaser is a person whose possession of a firearm would be unlawful. Consequently, if the prospective purchaser is using a fictitious identity, as our investigators did, an instant background check is not effective.

Our border security tests, in which we used counterfeit driver's licenses to enter the United States from various Western Hemisphere countries, point to the same problem. Because immigration regulations do not require U.S. citizens traveling from countries in the Western Hemisphere to show passports when entering the United States, persons entering the United States from such countries commonly present driver's licenses to border inspectors for identification purposes. However, border inspectors currently have no way of checking with the states to verify identity or to determine whether a driver's license is authentic.

Conclusion

A driver's license is the most commonly accepted document used to identify an individual. The weaknesses we found during these investigations clearly show that border inspectors, motor vehicle departments, and firearms dealers need to have the means to verify identity

[2] 18 U.S.C. § 922(t).

and to determine whether out-of-state driver's licenses presented to them are authentic. Improved verification procedures could minimize vulnerabilities presented when government officials do not recognize counterfeit documents or are not alert to the possibility of identity fraud. Also, government officials who review identification documents need training and need to be more vigilant for identification fraud.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other members of the committee may have at this time.

Contacts and Acknowledgement

For further information regarding this testimony, please contact Robert Cramer, Managing Director, or Ronald Malfi, Director, Office of Special Investigations at (202) 512-6722. Individuals making key contributions to this testimony include Dan Bertoni, John Cooney, Jennifer Costello, Barbara Lewis, and George Ogilvie.

Appendix I

Summary of Recent Reports and Testimony

Security: Vulnerabilities Found in Driver's License Applications Process

From July 2002 through May 2003, Office of Special Investigations (OSI) investigators visited state driver's licensing agencies (hereinafter referred to as DMVs) in Virginia, Maryland, the District of Columbia, South Carolina, Arizona, California, Michigan, and New York. Because the focus of this test was to determine whether DMVs would issue driver's licenses based on counterfeit documents, we obtained valid undercover Social Security Numbers (SSN) from the Social Security Administration (SSA) that would be verified by SSA if queried by DMV employees.[1] We were successful in obtaining authentic but fraudulent driver's licenses using fictitious names supported by counterfeit documents, including counterfeit out-of-state driver's licenses. We used the same fictitious names, birth dates, and SSN's at most of the locations without detection, and we used the same counterfeit driver's licenses in all states except Maryland and Virginia.

During the course of this investigation, we found that DMV employees generally did not recognize our counterfeit driver's licenses. Other DMV employees recognized irregularities in the documents we submitted but they routinely returned the documents to us. This investigation revealed that the current system in the 26 states that rely solely on visual inspection of documents to detect counterfeits is vulnerable and can easily be exploited.[2]

[1] SSA provides a verification service that allows state DMVs to verify the name, SSN, and date of birth of an applicant. While 26 states, including one state we visited, rely primarily on visual inspection of documents submitted by driver's license applicants to detect counterfeits, 24 states and the District of Columbia now use SSA's verification service. Nevertheless, criminals can steal the identities of individuals and obtain driver's licenses using counterfeit documents containing those individual SSNs. In addition, our investigative work has demonstrated that criminals can create documentation for fictitious individuals and apply for and receive valid SSNs, which can be used on counterfeit documents to obtain a driver's licenses.

[2] GAO-03-989RNI.

Social Security Numbers: Ensuring the Integrity of the SSN

In May 2003, we were able to prove the ease with which individuals can obtain SSNs by exploiting SSA's current processes. Working in an undercover capacity, we used counterfeit identification documents to obtain valid SSNs from SSA for two fictitious infants. By posing as parents of newborns, we obtained the first SSN by applying in person at a SSA field office using a counterfeit birth certificate and baptismal certificate. Using similar documents, we obtained a second SSN by submitting the counterfeit documents through the mail. In both cases, SSA staff accepted our counterfeit documents as valid. Thus, SSA's current policies relating to issuing SSNs to children under the age of one expose the agency to fraud.[3] SSA officials stated that they are reevaluating their policy.

During a hearing on July 10, 2003, we discussed our visits to DMVs in two states where we obtained authentic but fraudulent driver's licenses using the names, SSNs, and dates of birth of individuals listed on SSA's Master Death file. The Master Death file is publicly available and contains SSN's of deceased individuals. The two states we visited are among several states that rely on visual verification of identification documents and use SSA's batch process verification service, which allows DMVs to verify the name, SSN, and date of birth of an applicant but does not check the applicant's information against SSA's Master Death file.[4] Further, our analysis of 1 month of transactions submitted to SSA by one of these states showed that driver's licenses and identification cards had been issued to 41 individuals who used the names, SSNs, and dates of birth of persons listed as deceased in SSA's records. Our ability to obtain driver's licenses in the two states we visited and the 41 cases identified in our analysis demonstrate a significant gap in SSA's verification service to the states.

[3] U.S. General Accounting Office, *Social Security Numbers: Ensuring the Integrity of the SSN*, GAO-03-941T (Washington, D.C.: July 10, 2003).

[4] SSA also offers an on-line process to states that includes matching the applicants' information against the Master Death file.

Counterfeit Documents Used to Enter the United States from Certain Western Hemisphere Countries Not Detected

From September 2002 through May 2003, we used counterfeit documentation, including counterfeit driver's licenses and fictitious names, to enter the United States from Jamaica, Barbados, Mexico, and Canada. Bureau of Immigration and Customs Enforcement (BICE) staff never questioned the authenticity of the counterfeit documents, and our investigators encountered no difficulty entering the country using them. Although BICE inspects millions of people who enter the United States and detects thousands of individuals who attempt to enter illegally each year, the results of our work indicate that BICE inspectors are not readily able to detect counterfeit identification documents.[5]

Security Breaches at Federal Buildings in Atlanta, Georgia

In February and March of 2002, we breached the security of four federal office buildings in the Atlanta area using counterfeit law enforcement credentials to obtain genuine building passes, which we then counterfeited. In addition, we were able to obtain building passes that indicated that we were authorized to carry firearms in the buildings. As a result, several investigators, including one carrying a briefcase or package, bypassed the magnetometers and X-ray machines and used the counterfeit building passes to enter several buildings. They were able to move freely and extensively throughout these facilities during day and evening hours and were not challenged by anyone. In addition, they obtained a security guard's after-hours access code when they presented the counterfeit building passes.

[5] U.S. General Accounting Office, *Counterfeit Documents Used to Enter the United States from Certain Western Hemisphere Countries Not Detected*, GAO-03-713T (Washington, D.C.: May 13, 2003).

During this investigation we found that these buildings had security systems in place to screen visitors and valises. These systems included the use of magnetometers and X-ray machines at security checkpoints. The security systems also required that employees wear building passes for identification, which allowed them to bypass the magnetometers and X-ray machines. However, we were able to gain access because the employee responsible for issuing building passes did not follow existing procedures to verify the investigator's identity. Further, other security personnel failed to identify the counterfeit building passes. The Federal Protective Service, which is responsible for security at federal buildings, took action as a result of the weaknesses we identified.[6]

Firearms Purchased from Federal Firearms Licensees Using Bogus Identification

From October 2000 through February 2001, we used counterfeit driver's licenses with fictitious identifiers to purchase firearms from federal firearm licensees in five states—Virginia, West Virginia, Montana, New Mexico, and Arizona. The weapons purchased included (1) a 9mm stainless semiautomatic pistol, (2) a .380 semiautomatic pistol, (3) a 7.62mm Russian-manufactured rifle, (4) a .22 caliber semiautomatic rifle, (5) a 9mm semiautomatic pistol, and (6) a .25 caliber semiautomatic pistol.

The five states in which we purchased firearms conformed to the Brady Handgun Violence Prevention Act of 1993[7] by requiring instant background checks. For the most part, the federal firearm licensees we contacted adhered to then-existing federal and state laws regarding such purchases, including the instant background checks. Because we used counterfeit driver's licenses and fictitious identities there was no negative information in the system about the names we created.[8]

[6] U.S. General Accounting Office, *Security Breaches at Federal Buildings in Atlanta, Georgia*, GAO-02-668T (Washington, D.C.: Apr. 30, 2002).

[7] 18 U.S.C. § 922(t).

[8] U.S. General Accounting Office, *Firearms: Purchased from Federal Firearm Licensees Using Bogus Identification*, GAO-01-427 (Washington, D.C.: Mar. 19, 2001).

Purchase of Firearms Using a Counterfeit Federal Firearms License

In January 2002, we purchased a firearm from a licensed federal firearms dealer using a counterfeit federal firearms license. We established a fictitious sporting goods company in Virginia by using a legitimate federal firearms license and altering it to insert the name and address of our fictitious business. We then contacted a legitimate federal firearms dealer in Texas, posing as an individual wanting to purchase a .32 caliber semiautomatic pistol and have it shipped to Virginia. When the dealer stated that he could only mail the pistol to another federal firearms licensee, another investigator called the dealer, represented himself to be a licensed federal firearms dealer, and faxed a copy of a counterfeit license. The Texas dealer accepted the license and mailed the pistol. We also reported on two instances in which individuals purchased firearms using counterfeit or altered federal firearms licenses.[9]

Security: Breaches at Federal Agencies and Airports

In April and May of 2000, OSI investigators breached security at 19 federal sites and 2 commercial airports. Our investigators carried bogus badges and credentials, declared themselves to be armed law enforcement officers, and gained entry while avoiding screening procedures, including magnetometers and X-ray machines. At least one investigator carried a valise. Sixteen of the sites contained the offices of cabinet secretaries or agency heads. At 15 of these sites, investigators were able to stand immediately outside the suites of the cabinet secretary or agency head. In five instances, we were able to enter the cabinet secretary or agency head's suite. At the two airports we visited, investigators used tickets issued in fictitious names, declared themselves to be armed law enforcement officers, displayed their spurious badges and identification, and were issued "law enforcement" boarding passes by airline representatives. They then went to the security checkpoint and were waived around the magnetometers. Their valises were not screened. These investigations took place before September 11, 2001. Subsequently, federal agencies changed their policies to address the weaknesses we demonstrated.[10]

[9] U.S. General Accounting Office, *Purchase of Firearms Using a Counterfeit Federal Firearms* License, GAO-02-383R (Washington, D.C.: Mar. 13, 2002).

[10] U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, GAO/T-OSI-00-10 (Washington, D.C.: May 25, 2000).

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Testimony of Robert Douglas
Before the
United States Senate Committee on Finance
--
Hearing on
Homeland Security Threats Posed By Document Fraud,
Identity Theft, and Social Security Number Misuse

September 9, 2003

Introduction

My name is Robert Douglas and I am the CEO of American Privacy Consultants, Inc. (APC). APC provides consultation to the private and public sectors on issues involving all aspects of identity theft and identity fraud. During the past five years my work has centered on assisting the financial services industry, government, and law enforcement agencies to better understand the scope and methodology of identity crimes through educational materials, presentations, auditing, and consultation. Additionally, I have provided consultation and expert testimony for civil and criminal investigations brought by private parties and state and federal law enforcement agencies.

I have testified before the United States Congress on three previous occasions. The July 28, 1998 Hearing on "The Use of Deceptive Practices To Gain Access To Personal Financial Information" (U.S. House of Representatives Committee on Banking and Financial Services); the April 12, 2000 Hearing on "Establishing a Commission For the Comprehensive Study of Privacy Protection" (U.S. House of Representatives Committee on Government Reform, Subcommittee on Government Management, Information and Technology); and, the September 13, 2000 Hearing on "Identity Theft and Related Financial Privacy Issues" (U.S. House of Representatives Committee on Banking and Financial Services).

In addition to my previous testimonies before Congress, I served as a consultant and expert witness for the Federal Trade Commission in the preparation and execution of Operation Detect Pretext, a sting operation designed to catch and prosecute individual and corporate offenders participating in the illegal "information broker" industry. I also served as an expert witness to the Florida Statewide Grand Jury On Identity Theft. I continue to serve as an expert witness and consultant for the plaintiffs in a federal civil action brought in New Hampshire by the parents of Amy Boyer, a young woman slain in a murder/suicide committed by a man who purchased Ms. Boyer's social security number, date of birth, and place of employment from a web-based information broker. I have lectured before local, state, federal and international law enforcement associations on the topic of identity crimes.

To assist the private sector and the financial services industry in its' efforts to detect and combat financial crimes involving identity theft, I have authored a number of training

guides including: "Privacy and Customer Information Security – An Employee Awareness Guide" (2001); and, "Spotting and Avoiding Pretext Calls" (2000). I have served as a keynote speaker for the FDIC and I have been a frequent lecturer at state and national banking association conferences.

Finally, prior to founding American Privacy Consultants, Inc., I was a Washington, D.C. private detective specializing in criminal defense investigation. I have worked cases involving murder, international terrorism (including conspiracy to murder U.S. nationals and hijacking), political corruption, and government fraud. I have twice been appointed by the U.S. District Court for Washington, D.C. to serve as criminal defense investigator in matters involving international terrorism by members of known Islamic terrorist organizations.

The GAO - OSI Investigation
Problems Presented

There are many troubling issues raised by the General Accounting Office – Office of Special Investigations' report made public today at this hearing.

The now documented fact that a terrorist could potentially walk into a DMV licensing office and present obviously fraudulent documents in exchange for a driver's license - thereby increasing the probability of boarding an aircraft just as the September 11th terrorists did - shocks the conscience.

But the extent of the problem does not end there.

The same fraudulently obtained driver's license could assist terrorists or other criminals to gain access to secure government and/or private facilities in order to perform a myriad of criminal activities ranging from surveillance and reconnaissance to actual criminal or terrorist acts.

Additionally, the same fraudulently obtained driver's license could assist a terrorist or other criminals to open a financial services account; transfer funds in or out of the country; launder money; or, steal the funds of a legitimate account holder.

The GAO report shows that no exceptional means or methods were used by OSI agents to deceive DMV officials. To the contrary, the fraudulent documents were prepared using equipment and software available to any individual in the world. In the final analysis, the fraudulent documents used by the GAO undercover agents were of lesser quality than a terrorist or identity criminal could and would be expected to use.

The fact that a number of DMV officials did not even question the fraudulent documents presented by the agents is inexcusable, but sadly, not unexpected.

Prior GAO investigations and subsequent congressional hearings have revealed that in far too many aspects we are a country lax in security. Let me cite one example.

GAO agents, posing as law enforcement imposters, previously demonstrated their ability to gain access to highly "secure" areas of federal buildings and airports by merely flashing bogus movie-prop badges and fraudulent identification cards available to any terrorist or criminal via mail or the Internet. Having gained access to these "secure" facilities while armed with handguns, GAO agents were able to simulate leaving bombs in areas that would have had grave impact upon our national security structures and personnel had the bombs been real.

Time and time again, facility penetration tests and tests of identification authentication protocols in both the private and public sectors have resulted in what can only be called absolute failure. That is again the case today when it comes to the ability of state DMV's to adequately determine the legitimacy of documents presented during the issuance of the most heavily relied upon form of identification in America today.

Indeed, my own experience in training and auditing bank employees and identification authentication systems teaches me that far too many financial services companies, called by President Bush the nation's first line of defense in stopping the movement of terrorist funding, are woefully inadequate in their ability to provide that defense.

There are several significant reasons for this failure: The lack of standardized identification authentication equipment and systems; the lack of appropriate security protocols within the institution; the lack of adequate training of existing protocols; and, the poor performance by individual employees in following security protocols that have been provided and trained.

While the majority of my first-hand experience is based upon teaching, training, and auditing authentication systems within the financial services sector, there is no reason to doubt that the same lessons learned are applicable in all private and public organizations.

Experience also teaches that the "perfect" identification authentication system does not exist, nor will it ever. Any equipment or system designed can be beaten in one fashion or another. But it is foolhardy not to have the best system available and economically feasible. Clearly, that is not the case when it comes to DMV authentication procedures and protocols.

It would not be a surprise that DMV officials could be deceived with high quality fraudulent documents. It is of great concern that obviously fraudulent documents of relatively poor quality were, in a number of the tests, accepted without question. Further, the apparent lack of standardization in reviewing the fraudulent documents and the lack of reporting or seizure of detected fraudulent documents is a glaring deficiency that must be addressed.

Let me place as much emphasis as possible on that last point – one that I find most disturbing and needing immediate correction. The fact that any state DMV official would allow an individual presenting questionable or obviously fraudulent documents to leave the DMV facility still in possession of the fraudulent documents is mind-boggling in either a pre or post 9/11 environment.

The Broader Issue

Just this past week, the Federal Trade Commission (FTC) released a new survey showing that upwards of 27 million Americans have been victimized by identity theft in the last five years. According to the study, 10 million were victims in the last year alone.

The FTC's report also paints a grim picture of financial losses due to identity theft. Forty-eight billion dollars to the financial services industry and five billion in losses to individual Americans should ring out across America as loud as the loudest bank hold-up alarm manufactured. For that is precisely what this is – a national bank robbery underway right before our eyes.

The responsibility and damage caused to citizens and the U.S. economy at large by identity theft and subsequent financial fraud is properly placed at the feet of the criminals themselves. But common sense dictates that if the financial services sector was doing a better job of protecting funds we wouldn't be seeing fifty-three billion dollars in losses per year. Identity theft and financial fraud are (like so many other crimes) crimes of opportunity. As a nation we must take steps to reduce opportunities, aggressively pursue identity criminals, and severely punish those who are convicted of identity crimes.

While the numbers are staggering, they do not come as a great shock to those of us who have been following the issue for years. Many of us following identity theft trends had placed the cases per year number at 700,000. I was pleased to see Attorney General Ashcroft accept and endorse that figure two years ago at a press conference when he identified Identity Theft as the fastest growing crime in America.

We now know based upon the FTC survey and two recently released private sector surveys that the 700,000 victims per year figure was dramatically low. Again, this is not a surprise.

The anecdotal evidence has been present for years that this is not just another crime in the United States. Indeed, if identity theft were an illness, it would be a plague of Biblical proportion. Time and time again when I ask audiences at conferences and training seminars if they or a family member have been a victim of identity theft in the recent past, more than 50% of the participants raise their hands. It is not a statement of exaggeration to say that everyone in America has been or knows a victim of identity theft. I doubt there is a single other crime that statement would be applicable to.

The obvious question is: What is feeding the ease with which identity theft and identity fraud crimes are carried out? The answer is multi-faceted but straightforward.

First - Ease of access to biographical information of all Americans.

Second – Lack of standardization in identity documents and authentication protocols.

Third – Ineffective authentication protocols and training.

I. Access To Biographical Data On All Americans
The Illegal Information Broker Industry

As was crudely demonstrated by a California special interest group several weeks ago outside the White House, information about all Americans is easily obtained for free or for a small fee. As part of the publicity stunt, the group demonstrated that they were able to purchase the social security numbers of the Director of Central Intelligence and the Attorney General, amongst others.

While crude, the point is well made. If the highest public officials of our country can have their social security numbers sold on the web like Elvis memorabilia on E-Bay, what chance does everyone else stand at protecting their identity. After all, the social security number is the key that opens the kingdom for identity thieves.

But the demonstration, while successful in getting the media's attention, dramatically understated the problem. The sale of SSN's on the World Wide Web is just the tip of the iceberg.

The reality is anyone can buy the following: SSN's; dates of birth; home and work addresses; phone numbers; mother's maiden name; DMV information (including license plate numbers, driving histories, and specific vehicle information); floor plans of homes and businesses; voter identification information; bank account numbers and balances; investment portfolio details; telephone and cellular phone records (including specific numbers called); medical records; phony identification documents including accurate reproductions of driver's licenses and other forms of state or federally issued identifications; credit card transaction records; and, even the equipment to create or steal information from or for "secure" magnetic card stripe credit cards and identification cards.

That's a partial list.

Enterprising criminals calling themselves "information brokers" can access anything about anybody in any database. Having accessed the information they sell it on the Internet, in yellow page ads, in the back of trade journals, or in the underground information black market.

I have appended to my testimony (Appendixes A & B) my two previous congressional testimonies before the then House Committee On Banking And Financial Services, documenting in great detail the extent of the illegal information market in America.

While some of the specific examples and companies named in the prior testimonies may have ceased their practices, the techniques documented remain current and growing in scope and sophistication.

For the sake of illustration, I'd like to draw the Committee's attention to a web site called Hackers Home Page and available for viewing at www.hackershomepage.com On the left hand menu of the site is a section titled Catalog. Under Catalog is item #6, Magnetic Stripe/ID Cards. Within that section is all the equipment, software, and material needed for a sophisticated and/or organized identity theft and financial fraud operation. The site has a number of disclaimers regarding illegal activity that boils down to "Don't Ask – Don't Tell". In essence, anyone can buy these products and put them to use.

I have monitored the illegal information market for six years now on a daily basis. I read Internet chat room, newsgroup, and bulletin board postings and discussions of those actively involved as information brokers. While a significant number of information brokers and private investigators who once traded in illegal information have decided to comply with state and federal laws, many openly scoff at Congressional and law enforcement attempts to curb the trade.

The sad reality is the illegal information market is as healthy as ever. The proof is reflected in part by the staggering identity theft numbers released by the FTC last week. In every investigation of an information broker I have been involved with, whether a private lawsuit or law enforcement investigation/prosecution, there has been evidence of the information broker being used by identity thieves.

It is this ease with which identity thieves, and by extension, every criminal and terrorist in the world can obtain the information needed to assume the persona of any American in order to disguise criminal or terrorist activity. The ability to obtain a state issued driver's license in the name of another is a small but significant outcome of the overall identity theft problem.

II. Lack Of Standardization
Identity Documents and Authentication Protocols

One need go no further than the GAO report presented today to understand that we have a dizzying array of forms of officially distributed state DMV driver's licenses; forms of underlying documents accepted by DMV's for issuance of those licenses; DMV authentication protocols; and, adherence and use of existing authentication protocols.

In fact, I have recently seen it reported that there are currently 400 official formats of state issued driver's licenses and non-driver identification cards. That number seems impossible until you take into consideration that there are 50 states that issue licenses and non-driver ID's. To those 100 formats you add the fact that as the formats are changed for security or style reasons by each state, the older formats are not recalled.

The end result is simple. Hundreds of officially issued state identifications that no one in the United States can conceivably determine the validity thereof with any degree of certainty and consistency. Yet that is precisely what stands between the next Mohammad Atta and access to a U.S. based airliner today.

Compounding the problem presented by the variation in current state issued identification documents is the equally dizzying variation in underlying documentation accepted for the issuance of the state license or ID. These documents include, but are not limited to social security cards, birth certificates, foreign and domestic passports, green cards, and foreign matricula consular cards.

As if that were not enough, add the fact that there are no reliable and/or secure methods for determining the authenticity of any of the documents described so far.

We will never get a handle on the identity fraud epidemic in this country absent some form of standardization of documents accepted for issuance of a driver's license or other forms of identification; standardization of licenses and identifications issued; and, standardization of equipment and protocols for determining the validity of documents.

Bottom line. It really is quite simple. In the United States today we have a state issued identification system predicated upon a fiction and built upon a fallacy.

The fiction is the belief that current state issued identification systems afford us a level of security.

The fallacy is the belief that state issuing officials can - and will with certainty - issue license or identification cards to only the individual named on the license or ID card.

III. Ineffective Authentication Protocols And Training

Here again one look no further than the GAO report to recognize that document authentication protocols are inadequate and/or non-existent and training to existing protocols is insufficient.

The worrisome fact that a number of state officials did not recognize the presented documents were fraudulent demonstrates the lack of appropriate authentication protocols; the lack of available authentication systems; the lack of training to available systems and protocols; or, perhaps all three depending upon the individual state.

As previously noted, the most worrisome factor of all is that a number of officials did recognize the documents as fraudulent, but proceeded to allow the GAO undercover agent to leave with the fraudulent documents and absent any apparent notification of appropriate law enforcement or even supervisory officials.

Indeed, the attitude of issuing officials appears to be one of customer service first, security second – or perhaps last.

I have seen this problem on an almost universal basis during my work with the private and public sector. For much of corporate and governmental America, customer service comes before common sense security. That was acceptable in many ways prior to 9/11. It is not today. Security must stop being an afterthought that is viewed by corporate America and our government agencies as an albatross that either does not contribute to the bottom line or takes away too many dollars from other government programs.

I will again turn to my experiences with the banking industry as an example. In almost every conversation I have with banking officials who work in the compliance or security divisions of their institutions, complaints are raised that they are not given the resources, cooperation, or respect for their responsibilities within their institution. In a world where there is evidence that terrorists are using identity theft combined with financial fraud to fund terrorist operations with stolen American dollars, this laissez faire attitude in the financial services sector must cease.

A small but significant case in point. In July of 1998 I testified before Congress on the need for banks to use personal identification numbers (PIN's) instead of biographical data like mother's maiden name or the last four digits of the SSN to secure banking by phone systems. In fact, the acting Comptroller of the Currency was sitting behind me taking notes. After the hearing, the OCC, followed by the other banking regulatory agencies put out official advisory letters to all banks in the nation suggesting they utilize PIN's (in addition to a number of other suggestions made to reduce financial fraud as a result of identity theft).

To this day, there are hundreds upon hundreds of banks in America that an identity thief, armed with the biographical data of a legitimate bank account holder, can steal money out of an account by phone. Simply because the bank refuses to change the authentication protocol from a biographical fact that any thief can purchase on the Internet, to a PIN only known by the account holder. This is not theory. It has happened time and time again with some very prominent Americans being the victims of bank robbery by phone. It may be the easiest crime in America today.

While that is one glaring example, it is not the only one. Further, the problem, as demonstrated by the GAO report released today, is not confined to the financial services industry. It is an American problem. It pervades every private and public sector. It is a problem of attitude and determination. Having the attitude to accept the need for effective authentication protocols combined with the determination to see the protocols trained and followed to the degree needed for effectiveness.

Thankfully, we have historically had a country where security did not need to be paramount in our thinking and daily business and government practices. Unfortunately - as demonstrated by 9/11, the recent FTC survey, and many other daily examples and reminders - those carefree days are gone.

Considerations and Recommendations

Given the problems revealed by the GAO – OSI report concerning state DMV's ability to detect fraudulent documents I would place for consideration the following recommendations:

1) Audit Of Existing State DMV Protocols: To determine the full scope and variation of state protocols in reference to accepting underlying documentation for issuance of driver's licenses and non-driver's identification cards, an audit of every state's protocols should be performed.

2) Standardization Of Driver's Licenses And Non-Driver's Identification Cards: Agreement and acceptance by all states of a secure, standardized format for state issued driver's licenses and non driver's identification cards would facilitate ease of authentication by one state of another state's license or identification card.

3) Standardization Of Proof Of Identity Authentication Documents: Agreement and acceptance by all states of underlying proof of identity authentication documents (such as birth certificates and passports) required for the issuance of a driver's license or non-driver's identification card would restrict forum shopping by identity thieves and reduce the number and variety of documents currently presented.

4) Reduction Of Acceptable Proof Of Identity Authentication Documents: Reduction and restriction of currently acceptable proof of identity documents such as the non-secure and unverifiable matricula consular card cited by the FBI as a threat to national security, the non-secure and easily replicated social security card, employment identification cards, utility bills, and rental contracts, would reduce the number of documents examiners are responsible to recognize the authenticity of.

5) Standardization And Addition Of Security Features For Birth Certificates, Passports, And Other Proof Of Identity Document: Standardized biometric or other agreed upon security features added to birth certificates, passports, or other agreed upon proof of identity documents would enable each state or jurisdiction to authenticate another state's or jurisdiction's forms of identification, while maintaining state control of issuance and data storage.

6) Legislation Making Presentation Of Fraudulent Documents In An Attempt To Obtain A State Or Federally Issued Form Of Identification A Federal Crime: If current state and federal laws are deemed inadequate, consideration should be given to creating a federal criminal statute specifically addressing the presentation of fraudulent documents to a state or federal agency in an attempt to obtain a state of federal form of identification.

7) Regulation Requiring State DMV Officials To Seize And Report Fraudulent Documents: Consideration should be given to adding or upgrading existing federal

regulations requiring state DMV officials to seize suspected fraudulent documents and report individuals presenting the documents to federal law enforcement.

8) Regulation Requiring Personal Identification Numbers (PIN's) For Consumer Access To Any Financial Services Industry Records: Access by consumers to any and all financial services industry records must require use of a PIN or non-biographical identifier. This is already required for the use of ATM cards and many credit card transactions, yet many bank by phone transactions and inquiries can be performed by providing biographical information such as social security number, date of birth, mother's maiden name, or combinations thereof. Identity thieves and information brokers have easy access to biographical information and routinely defeat authentication systems using biographical identifiers.

9) Legislate Or Regulate The Sale Of Social Security Numbers: The sale of social security numbers must be restricted to appropriate uses such as fraud detection and prevention. The wholesale availability of social security numbers (and other biographical data) via the Internet, and other commercial means, is a threat to all Americans.

Appendix A

Statement by Robert Douglas

before the

Committee on Banking and Financial Services
United States House of Representatives

Hearing On
The Use Of Deceptive Practices To Gain Access To
Personal Financial Information

July 28, 1998

Introduction

Thank you, Mr. Chairman. My name is Robert Douglas and my firm is Douglas Investigations. My firm provides private investigative services to the Washington, DC legal community. While we specialize in complex criminal defense matters, we also provide general investigative services including traditional areas of civil investigation and information search services. It is my experience with the information broker industry that brings me before you today.

First, Mr. Chairman, let me state that I appreciate the opportunity to appear before you

to give my perspective on what I believe to be one of the most significant problems facing our nation today. I want to personally thank you for your willingness and desire to address this serious issue and the time you have invested on this problem. I am aware from both the legislation you have introduced and your public comments that you share my concerns about maintaining citizen's financial privacy. I particularly want to thank your Committee's staff, and specifically David Cohen, for the time they have invested with me discussing this problem.

Mr. Chairman, I also would like to single out for recognition your administrative assistant, Bill Tate, for his assistance in getting this critical issue before you and the Committee. When I first approached Bill with my concerns about this subject, he immediately recognized this as an issue worthy of you and your Committee's attention and moved quickly to bring it before you. For that I am thankful and I believe the American people will be thankful when they learn the scope and dimensions of the problem we are hear today to discuss.

All across the United States information brokers and private investigators are stealing and selling for profit our fellow citizens personal financial information. The problem is so extensive that no citizen should have confidence that his or her financial holdings are safe.

The types of financial information for sale include: Private bank account numbers and balances; stock, bond and mutual fund holdings including the number of shares held; insurance policy data including the types of insurance maintained and the amount or value of the policy; credit card information including account numbers, size of credit lines, and transaction details including specific purchases.

While the theft and sale of this information is occurring on a daily basis, much of societies focus on privacy as it relates to personal information has been concentrated elsewhere. To date, the majority of public scrutiny has been on issues related to basic data collected via the Internet and the explosion of information that is collected everyday as part of routine commercial transactions.

Issues such as the mass collection of citizens social security numbers, home addresses, phone numbers, and purchasing preferences by retailers have dominated the debate. As part of this debate we routinely hear and read of generic "what ifs..." and concerns that "sometime in the near future" a citizen's most privately held information will be easily obtained by anyone willing to pay for it.

Mr. Chairman, I am here today to tell you that we passed that point long ago and somehow it seems no one noticed.

The Sale of Financial Information
by "Information Brokers"

Currently, thousands of information brokers and private investigators are advertising their ability to locate citizen's personal financial information. The advertisements almost uniformly refer to "bank account searches" and/or "asset investigations". These advertisements can be found in legal and investigative trade journals, general circulation newspapers, the yellow pages, and on the World Wide Web.

The genesis of this specialty niche within the information industry is a growing black market that has developed to sell financial and other forms of personal information. As with most black markets, there needs to be a seller of a commodity that can't be obtained through normal channels and a buyer interested in that commodity. In this case the sellers are private investigators and information brokers, who I will collectively refer to as brokers, who have perfected a technique they call "pretexting". The commodity is private financial information. Originally, and to a great extent still, the buyers were lawyers looking to seize assets of individuals with unsatisfied judgments.

I do not want to mislead the Committee on this point. There is a substantial problem in this country concerning the ability of successful parties to a lawsuit ever collecting the monetary awards from the opposing party. There are millions of uncollected judgments representing billions of uncollected dollars in the United States. In my opinion, this fact has played a large role in the development of the black market for financial information. Indeed, if you review the materials I have provided to the Committee, most brokers providing these asset location services advertise them as a means to locate liquid assets to seize in order to satisfy judgments. However, if you review those materials closely in conjunction with the audio and video tapes I have provided the Committee of a private investigator and an information broker selling an individuals banking information, you will clearly see that far too many brokers are selling citizens private information to anyone who cares to purchase it.

Even if, for arguments sake, all brokers were only providing financial information obtained through pretext to attorneys holding lawful judgments as a means to assist in the collection on those judgments, it would still be a gross violation of privacy and in many states a violation of the law. In other words, in a society governed by law, the end cannot justify the means.

Yet this is the very argument that many brokers I have talked to make. Their position is that there is nothing wrong with what they do. They see themselves as financial bounty hunters filling a demand for information on where individuals have secreted their money. Time and again in numerous conversations I have had with brokers around the country I have heard the following two positions argued as a justification of the services they sell.

The primary position is that it is not against the law to obtain private financial information. In the materials I have provided the Committee there are two specific examples of this declaration. One is direct and the other is by inference. The first is a broker assuring the viewers of the web page that it is legal to obtain financial information. The second is a law firm newsletter on the web where they advise their

readers and clients that they use brokers to locate bank accounts and that they will assist their clients in hiring brokers to do the same.

In furtherance of this position that what they do is legal, brokers argue that there is no federal law prohibiting a private citizen from obtaining the financial information of another private citizen. The brokers, and in some instances their corporate attorneys, have told me that federal laws in this area relate only to the government's access to a citizen's financial information. I would like to note that these very brokers and their attorneys appear to be ignoring existing state laws in many instances.

The second position brokers advance is that "pretexting", which I will discuss in more detail shortly, is perfectly legal. The argument goes like this. "If the bank is stupid enough to tell me the information, that's the banks problem--not mine."

The Extent of the Problem

Five years ago there were a small number of these brokers actively advertising their "asset location" services. The advertisements at that time were largely confined to legal and investigative trade journals, as the target markets were lawyers and creditors who had judgments that had remained uncollected.

Today, there are literally hundreds of brokers advertising around the United States by means of the Internet. By way of example I have provided to the Committee, and have here at the table with me today, approximately 285 individual web pages from approximately 40 companies advertising on the World Wide Web. These 40 companies were located by searching the phrase "bank account search" on just one of the many Internet search engines. Specifically, the AltaVista Internet search engine.

The results are a combination of information brokers and traditional private investigators. Each of these firms is advertising to other private investigators, information re-sellers, attorneys, and often the general public. Even the firms that are publicly stating that they are not selling to the public will gladly sell to a private investigator without any ability to control where the data will go from there. The end result is that thousands of investigators, brokers, and in many cases individual consumers can now purchase the personal financial information of any citizen in the United States.

To further illustrate to the Committee the scope of the problem we are discussing today I would like to point out another fact. By just examining two of the forty companies I have provided the Committee with web pages for, Noble Assets and The Pathfinder Group, you will see that they claim to have located over 1.5 billion dollars in assets. If we take them at their word, or even if we divide that number by a factor of two, the scope of the dilemma is staggering.

Identity Theft and Pretexting

The means by which private financial information is most commonly obtained is identity theft. The financial data is obtained by the broker under false pretenses. The most common method of identity theft used to obtain privately held financial information is for the broker to obtain through currently legal means enough biographical information on the target of the investigation to be able to falsely pretend that he, the broker, is the actual owner of the information sought after. Having convinced the financial institution by false pretenses that he, the broker, is actually the institution's client, the institution is only too happy to provide whatever information is requested.

The following is a basic example of this method. Bob Smith is the holder of a bank account at USA Bank. Joe Info Broker obtains from one of dozens of lawful databases, many of which can be found on the Internet, Mr. Smith's full name, social security number, address, and date of birth. Joe Broker then starts calling banks in Mr. Smith's neighborhood posing as someone who has received a check from Mr. Smith. When Joe Broker finds a bank that confirms that Mr.Smith has an account, Joe Broker hangs up. Joe Broker then calls back and identifies himself to the bank as Mr. Smith. The bank, for security reasons, asks for personal information that the bank mistakenly believes only Mr. Smith would know. Joe Broker armed with Mr. Smith's biographical data is able to convince the bank that he is actually Mr. Smith. The bank then provides Joe Broker with any information he requests on Mr. Smith's account.

A second method is for the broker to falsely convey to the target of the asset investigation that he, the broker, is an employee of a legitimate financial institution or company. Having gained the confidence of the target, the broker induces the target to provide his or her own financial data.

The following is a basic example of this second method. Joe Info Broker, having determined Sally Senior Citizen's bank by the means outlined above, calls Sally Senior Citizen at home and pretends to be an employee of the bank. Joe Broker tells Sally that there is some confusion with her account and that they can clear it up on the phone if she goes and gets her checkbook. Sally wanting to avoid a trip to the bank complies. Joe Broker having gained Sally's confidence gets her to read her account number to him as a means of "confirmation". Joe then gets Sally to tell him what her balance is so "the bank" can be sure its records are accurate. Sally complies. Joe Broker now has Sally's banking information.

These are just two of many methods that I have uncovered. I note that the Committee will hear today from an information broker, Al Schweitzer, and I suspect that Mr. Schweitzer will be able to provide other techniques commonly in use. However, at the core of any of these techniques is identity theft.

Private investigators and information brokers who obtain these types of information by the above methods prefer to call it "pretexting". While pretexting is a commonly accepted investigative technique, I believe it is more properly classified as fraud when it rises to the level of identity theft as outlined above.

Pretexting is a traditional, accepted investigative technique within the investigative trade. The technique of pretexting is to either intentionally induce or allow another party to believe the investigator is someone they are not. The goal being that the individual being pretexted will drop their guard and reveal information that they would not if they knew the true identity of the investigator. This technique is routinely used by both law enforcement and private investigators.

An example of traditional pretexting would be to pose by phone as a generic delivery person with a package for Mr. Jones as a method to determine if Mr. Jones is home so that a subpoena could be served or a warrant executed. A second example would be to pose as an "old school friend" in order to find the current address of Mr. Jones from Mr. Jones' parents. The goal again being to learn the public address of Mr. Jones so that lawful process can be carried out.

The difference between true pretexting and identity theft is simple. In pretexting, the investigator poses as a generic individual or company in order to obtain public, non-protected information such as an address, name of a witness or relative. Identity theft is the use of the targets personal and biographical information to impersonate the target as a means to obtain the target's private, protected information.

Creditor Networks and "Sources"

While I believe identity theft is currently the most common method being used by information brokers today, and is almost always used to gain the balance of a financial account, it is not the only method.

Creditor networking as a means of obtaining personal financial information is another method used by brokers. This method consists of a broker calling companies that have made inquiries on a target's credit report in order to learn what biographical and financial information that company maintains on the target. The broker will offer to exchange data in the broker's possession or promise to call back with information developed as a means to induce the company to provide personal data on the target. By calling one or more companies the broker begins to piece together the financial profile of the subject in order to then sell that information to the broker's client.

The final method I will address is that of using "sources". The term source in the investigative trade is often code language for illegally obtained information. The broker purchases or trades on an existing friendship or relationship to obtain protected information from the "source". Brokers spend years developing "sources" and are constantly trying to cultivate new ones to obtain information.

I have heard brokers brag of developing sources within the major credit agencies as a means of obtaining "no foot print" credit reports. A "no foot print" credit report is a report obtained on a target that doesn't leave a notation on the report's inquiry section recording who has obtained a copy of the target's report. Brokers also try to develop

"sources" within the financial services sector itself. One of the tapes I have provided to the Committee and to the FDIC is replete with discussions of sources developed within the financial industry.

Stalking, Theft, and Financial Terrorism

In my introduction today I stated, "[t]he problem is so extensive that no citizen should have confidence that their personal financial holdings are safe." Mr. Chairman, I am not an alarmist by nature and consequently I do not make that statement lightly. Frankly, I fought a battle within myself debating whether I should make such an incendiary charge. However, the statement is true and I would like to provide the Committee with one example of what I know has already transpired by this information ending up in the wrong hands. Further, I would like to warn the Committee of what can easily happen, and perhaps has already, if quick action is not taken.

I am personally aware of a case that a Maryland private investigative agency has worked on where a stalker has purchased by means of a private investigator and an information broker the personal information of a Virginia woman. This information included amongst other items her driving record and personal banking information. As a form of harassment, terror and demonstration of power the stalker proceeded to distribute this information to all the woman's neighbors in her community.

While this example is bad enough in and of itself, it is just a small taste of the harm that can and will occur with this type of information so widely available by means of the Internet.

With the financial information that can be purchased from a broker and the techniques that these brokers will teach to others and sell in books advertised on the Internet the following can be accomplished:

Theft

1) You can steal money directly from the bank account of a citizen by using tele-check type services to make purchases.
2) You can steal money directly from the bank account of a citizen by having the money wired from the account to another location.
3) You can steal money directly from the bank account of a citizen by using the account information to make purchases on the Internet.
4) You can use a citizen's credit card information to make purchases by phone or the Internet.
5) You can use investment information to cash in holdings to obtain the funds.
6) You can determine the insurance coverage's and policy amounts of a citizen and cash in certain types of policies.

Financial Terrorism

1) You can close a citizens financial accounts.

2) You can stop payment on checks the citizen has issued.

3) You can use the knowledge of financial holdings to assist in blackmail or kidnapping.

4) You can determine a business competitors financial holdings as a means to obtain a competitive edge.

5) You can close a business competitors accounts or place stops on checks issued to create havoc for the competitor.

These are just a few examples of the types of harm that can easily be visited upon a citizen or business. I note that one of the guests today is Evan Hendricks representing Privacy Times. I suspect Mr. Hendricks will be able to supply stories he is aware of and/or potential scenarios of how financial information in the wrong hands can cause incredible amounts of damage in a very short period of time. In fact, it is easier to cause the damage than it is to correct it once it has taken place.

The Proposed Legislation

One of the questions I was asked to address in your invitation letter, Mr. Chairman, was whether I thought existing Federal and state laws adequately safeguard citizen's financial information. Quite simply they do not.

I note that Massachusetts Assistant Attorney General Clements is on the witness list for today. I would also note that all of the companies the State of Massachusetts prosecuted are still in operation to the best of my knowledge. As one broker we caught on tape stated to me concerning the fine given to Noble Assets, ..."what's twenty to thirty thousand dollars when you're making a quarter of a million a year".

I would also like to state that I researched the issue of whether obtaining private financial information is legal off and on for more than four years. I found it hard to come to a conclusion based upon existing law and a review of law journals and books on privacy. While everything in my gut told me that this can't be right, I saw dozens of other companies advertising the ability to provide bank account and other financial information. Many of these advertisements appeared and continue to appear in the local legal trade journal, Legal Times. This paper is read in all the major law offices and I have seen it in the U.S. Attorney's office for the District of Columbia.

Indeed, an attorney representing one broker, Integrity National, told me that she had researched both the law and the methodology being used by Integrity and that what they sold was perfectly legal. Noble Assets prominently displays that one of the principles of the firm is an attorney. At one point I went to a legal conference here in the District of Columbia titled "Collecting On Judgments In DC, Maryland and Virginia." I asked two members of the panel, both attorneys, if they could provide assistance in this area and all I got in return was a blank stare. They stated that they did not know the answer to the question of legality.

Based upon my early research and discussions with brokers and their attorneys I purchased financial information on behalf of attorneys looking to collect on judgments for approximately 2 years. At the end of that period I had an experience with a broker that clearly revealed to me that he was obtaining the information through fraud. At that point I ceased purchasing financial information and put out a warning to all my clients that I believed brokers were stealing this information by means of identity theft.

The preceding paragraphs are meant to illustrate that it is not easy to determine what laws specifically apply in this area. Because of that reason and because of the scope and danger presented I believe there needs to be Federal law directly controlling the use of deceptive practices to obtain personal financial information.

I have had an opportunity to review the legislation introduced by Chairman Leach and I believe it directly and fairly addresses the problem we are discussing today. The legislation clearly evidences a thorough understanding of the issues presented and outlaws the use of identity theft or theft by false pretenses in the obtaining of financial information. I support the inclusion of both criminal and civil remedies as a means of enforcement.

I believe that passage of this law coupled with enforcement will almost immediately end the problem. As I reviewed web pages advertising the sale of financial information, many of which I have provided to the Committee, I was struck by the fact that without exception they all noted that in order to obtain a credit report the purchaser had to be in compliance with the Fair Credit Reporting Act. Brokers are terrified of being put out of business and/or sued for violating the FCRA. I believe similarly they will get the word quickly that identity theft, as a means of obtaining personal financial information, is no longer acceptable.

Enforcement of the law will require a minimal amount of resources. Specifically, a single federal agent with a computer, Internet access, fax machine and the skill to out pretext the pretexters as I did, could shut this industry down in a matter of months.

Education

Finally, the last area that needs to be addressed is education. No matter what happens today and whether or not this legislation passes, we must do all we can to educate the public, your fellow legislators, financial institutions, hospitals, universities, and any other company or institution that maintains private information about the dangers of identity theft. As I noted earlier there are individuals teaching classes and writing books on how to "pretext". We need to teach businesses, institutions and individual citizens what steps they can take to protect their ever decreasing privacy and their most valued information.

Conclusion

Mr. Chairman, I would like to once again thank you for the invitation to appear today. I have great confidence that the Committee recognizes the seriousness of the problem before it and the threat it presents to the integrity of all financial information.

As a child I was taught that the first role of government is to protect the people. This is an opportunity for this Committee and this Congress to do so. As a professional in the investigative trade I would ask you on behalf of the honest members of the profession that you stop the use of deceptive practices to access financial information. As a citizen of the United States I insist that you do so.

I will be happy to answer any questions the Committee has.

Appendix B

Statement by Robert Douglas

before the
Committee on Banking and Financial Services
United States House of Representatives

Hearing On
Identity Theft and Related
Financial Privacy Issues

September 13, 2000

My name is Robert Douglas and I am the co-founder and Chief Executive Officer of American Privacy Consultants, Inc. located in Alexandria, Virginia (www.privacytoday.com). American Privacy Consultants assists organizations and businesses understand and implement appropriate privacy policies, strategies, defenses, educational programs, training, and auditing.

I appreciate the opportunity to appear before this committee once again to address the issue of identity theft, "pretext calling", and other deceptive practices still in use by some "information brokers", private investigators, judicial judgment collectors and identity thieves to illegally access the personal and confidential information of customers of financial institutions. Unfortunately, in spite of the enactment of legislation drafted by this Committee to outlaw such practices, these methods not only survive but also continue to grow in volume, scope, and methodology.

Chairman Leach, I want to personally thank you and the Committee for your continued willingness and desire to address this serious issue first by crafting and passing much needed legislation and now in an oversight capacity. I am personally aware of the

amount of time the Committee members and staff have invested in this problem over the last three years and as a citizen applaud the Committee's willingness to tackle these issues.

I also would like to single out for recognition Jim Clinger, the Committee's Senior Counsel and Assistant Staff Director. Over the last three years I have had the unique pleasure of working with Jim on a regular basis and he is a true credit to this Committee and to the United States Congress. Above all he is a true gentleman.

Finally, I would like to thank John Forbes, Special Agent – United States Customs Service; and, Alison Watson, Professional Staff Member of the Committee for their work over the last month in preparation for this hearing.

H.R. 4311

Although I was specifically asked to address the use of pretext and other deceptive techniques to access confidential financial information, I would like to make a few brief observations concerning HR 4311.

There can be little doubt that identity theft is one of the fasting growing crimes in the United States today. Each year hundreds of thousands of Americans fall prey to identity thieves. The financial and credit damage implications are severe for the individual who is the victim of identity theft. Additionally, retailers and financial institutions suffer financial losses as a result of identity theft. Finally, the nation as a whole suffers in increased prices for retail products and financial services including the cost of credit.

The advent of the World Wide Web has brought increased opportunities for identity thieves through ease of access to personal, biographical data needed to perpetrate identity crimes and facilitates ordering merchandise absent a face-to-face encounter with a store clerk. These facts require that we examine areas of weakness that identity thieves exploit.

In 1998 I demonstrated for this Committee the ease with which an individual can purchase private and confidential financial information. It is even easier to obtain the name, address, date of birth, social security number, mother's maiden name, phone number, and often the employment of any individual in the United States today. All of this information is for sale on the web. In a nutshell, all the information needed to steal a citizen's identity and create financial havoc is available on the Internet for little or no cost.

The largest source of up-to-date personal, biographical information is credit bureaus. The sale and resale of credit header information by credit bureaus to private investigators, information brokers and judicial judgment collection professionals results in this information being accessible to anyone for a fee. This is big business. Several large companies make millions of dollars each year reselling personal information gathered by the credit bureaus.

When citizens apply for credit or enter into a credit transaction they do not know that their personal, biographical information is then resold to any individual with a few bucks and a web browser. If the level of trust in the Internet is ever to rise from the relatively low position it now occupies, the sale of personal information must be brought under control. A good place to begin is by curtailing the sale of credit header information absent a permissible purpose as defined currently within the FCRA. For that reason I believe Section 8 of HR 4311 is long overdue.

Pretext and other Deceptive Practices
July 1998 through September 2000

On July 28, 1998, while appearing before this Committee, I stated: "All across the United States information brokers and private investigators are stealing and selling for profit our fellow citizens personal financial information. The problem is so extensive that no citizen should have confidence that his or her financial holdings are safe." Sadly, I return today to inform this Committee that my statement of 1998 remains true today.

While the illegal access of financial information continues, progress has been made. When we last met in July of 1998 four steps were required in order to stop these practices. First, the financial services industry needed to understand and take affirmative steps to combat the threat posed by unscrupulous information brokers, private investigators, and identity thieves. Second, tough federal legislation was needed to outlaw the use of pretext and deception as a means to access confidential financial information. Third, appropriate federal regulatory agencies needed to create standards and regulations designed to assist institutions in the safeguarding of financial information and to reflect the legislative intent encompassed within any legislation enacted by Congress. Finally, aggressive prosecution of individuals and companies who steal, buy, and/or sell personal financial information was required to signal that the integrity of our nation's financial system is a law enforcement priority. The first three sides of the square have been completed.

The financial services industry has made significant progress in beginning to combat identity theft and pretext through a sober recognition that this is not a problem that can be ignored if the industry wishes to maintain a reputation for providing confidentiality to customers. This recognition has been acted upon through the use of training programs and educational materials to begin the education of financial services industry professionals to the threats posed by identity thieves of all types. Many financial institutions have begun to enact internal standards designed to identify and thwart the practices of identity thieves and infobrokers. Is there more to do? Absolutely. Is the financial services industry taking the confidentiality of the records it safeguards on behalf of customers seriously enough to continue to move forward in this area? I believe so.

This Committee and Congress moved quickly to pass legislation designed to punish those who would impersonate others in order to gain access to private financial records. With the passage of Gramm-Leach-Bliley, there is now federal law outlawing the use of

pretext and other deceptive techniques to gain access to personal financial information absent several narrowly defined and commonly misunderstood exceptions.

The federal regulatory agencies with direct supervisory function of the financial services industry moved quickly in 1998, by means of an advisory letter and other steps, to alert all institutions to the practices of identity thieves and information brokers. These same agencies are continuing as we meet here today to develop standards and regulations in keeping with the intent of Gramm-Leach-Bliley.

With the first three sides of the box either erected or under construction, it is now time to build the final wall through aggressive enforcement action. With the enactment of Gramm-Leach-Bliley last November, I assume that the Federal Trade Commission and appropriate criminal enforcement agencies are now preparing to use the tools Congress and the President handed them.

To my knowledge there has been one federal enforcement action brought by the FTC against an information broker. That civil action was begun prior to the enactment of Gramm-Leach-Bliley under laws designed to thwart "unfair and deceptive trade practices". Several states, notably Massachusetts, have aggressively pursued illegal information brokers. Again, these actions were taken prior to GLB and under state laws against illegal trade practices. It is time for tough nationwide enforcement of the civil and criminal provisions contained within Gramm-Leach-Bliley.

In the invitation letter I received from the Committee to testify today I was asked to specifically address three areas: 1) The extent to which the use of pretext and other deceptive means continue in spite of the passage of Gramm-Leach-Bliley; 2) The effectiveness of efforts by the financial services industry to deter and detect fraudulent attempts to obtain confidential account information; and, 3) Other threats to financial privacy emerging today.

The Extent To Which Deceptive Practices Continue Post Gramm-Leach-Bliley

The use of pretext and other means of deception to trick financial institution employees and customers into disclosing personal and confidential financial information that I testified about two years ago continue unabated. Books have been written about pretext to teach and share common methods. Discussion groups abound on the Internet with the trading of new and improved techniques almost on a daily basis. Classes are held in which pretext methods are shared for a price. The techniques are becoming more complex and refined.

Advertisements on the World Wide Web have doubled in the past two years. Here is a typical example:

Bank Account Search

Search Price
$249.00

Availability
National

Approximate Return Time
10-18 Business Days*

Requires
Subject's Full Name, Complete Street Address, Social Security Number*

Search Description
Given a Subject's full name, complete address and social security number, this search will return the bank name and address, account type, account number, (if available) and approximate current balance of all located personal accounts. We access a proprietary database and identify open accounts using the Subject's SSN, however this search will only identify accounts in the Subject's primary state the business resides. If you suspect accounts exist in more than the primary residing state, a separate search request for each state is required, and should include the Subject's address in that state.

***This search requires the Subjects social security number. If the SSN is unknown, we will find it for the purposes of this search but it will not be included in your search result.**

NOTE: This search uses the Subject's social security number as the account identifier, so only primary account holders are returned. Also, be sure to include any additional information you may have, such as the Subject's home & work telephone, birthdate, mother's maiden name, etc, in the additional comments section. This will greatly increase the odds of a successful search.

Responsible Purpose For Search
This search may return sensitive, confidential, and/or private information. For this reason, DOCUSEARCH.COM requires an explanation stating the purpose for requesting this search, its' intended use and supporting documentation. Additionally, we reserve the right to decline to perform any search which we deem not to be for a legitimate legal purpose or may cause emotional or physical harm.

ImportantDisclaimer
Financial searches are for informational purposes only, and are not acceptable as an exhibit or as evidence. Every effort is made to provide a complete & thorough search result. However, no method of research is 100% fool-proof and no firm can offer an absolute guarantee that every account will be found.

*This search requires many hours of research and can't be rushed, as we want to return thorough, accurate results. Therefore, this is an **approximate** return time. (End)

This advertisement is remarkable in many regards. The ad claims to "access a proprietary database and identify open accounts using the subjects SSN", yet "this search requires many hours of research and can't be rushed, as we want to return thorough, accurate results" and the search may require "10-18 business days". There is no proprietary database available to private investigators or information brokers that by use of the SSN (social security number) banking information can be obtained. In fact this ad used to say the company accessed a "federal database" to obtain the information.

The ad further states: "Also, be sure to include any additional information you may have, such as the Subject's home & work telephone, birthdate, mother's maiden name, etc, in the additional comments section. This will greatly increase the odds of a successful search." Why would a database accessed by SSN require this personal information? It wouldn't. But pretext does. Many financial institutions use the mother's maiden name as a password. Further, some institutions will ask for your home or work phone numbers to verify the account holder. Finally, the phone numbers are often required as part of a pretext contact made directly to the account holder.

The ad also states: "Additionally, we reserve the right to decline to perform any search which we deem not to be for a legitimate legal purpose or may cause emotional or physical harm." Perhaps this is an attempt to signify that a search request must satisfy GLB and other applicable State and Federal laws. Perhaps not. Here is the transcript of an email contact I had with Docusearch:

```
From:       DOCUSEARCH.COM
To:         email address deleted
Subject:    Re: Information Request
Sent:       Mon 3/20/00 1:41 PM

You will first have to locate his address in the current residence
state.  This may be accomplished with a Locate by Previous Address
Search.  Then you can order the Bank Account Search.

At 01:38 PM 3/20/00 , you wrote:
>------------Begin, Information Request from visitor-----------
>My Name Is : Rob Douglas
>My Email Address Is : (deleted)
>My Telephone Number Is : (deleted)
>My Question Pertains To :  Other: Explain Below
>Comments : I have a client who is owed a substantial amount of money
>by a potential defendant who left the area and closed his personal and
>corporate bank accounts.  I have an old home address for the potential
>defendant and know what state he moved to.  What searches would you
>recommend to locate the potential defendant and his personal and
>corporate bank accounts?
>------------End, Information Request from visitor -----------
```

The ">" portions represent the email I sent to Docusearch using their on-line request form. Three minutes later I received the reply that I could order the bank account search in a situation that would clearly be illegal under GLB if pretext were used.

I would hope that members of this Committee would find the services offered and language of the advertisements by Docusearch to be as disturbing as I do. I suspect many of the members of this Committee would wonder why this firm is allowed to operate in this fashion given the provisions of GLB and the applicable "unfair and deceptive trade practice" sections of Federal law. The excuse might be offered that this is just one company that no one in a position of responsibility to address these practices was aware of. That excuse would ring hollow.

Docusearch is the company that sold personal information concerning Amy Boyer to a stalker that resulted in the murder of Ms. Boyer and the suicide of the stalker. Amy's parents have testified before Congress and have been widely covered in the media. In fact, Amy's death has led to consideration of legislation by this Congress to outlaw the sale of social security numbers. Throughout all this attention Docusearch has made one change to the web site where it advertises. Docusearch no longer publicly advertises the sale of social security numbers. But Docusearch continues to do business selling personal and confidential information.

The attention to Docusearch does not end there. Docusearch was the cover story for Forbes magazine on November 29, 1999. This was seventeen days after President Clinton signed GLB into law. In the article Dan Cohn of Docusearch literally bragged about his abilities to obtain personal information about a subject. Here is the opening quote from the Forbes cover story:

THE PHONE RANG AND A STRANGER CRACKED SING-SONGY AT THE OTHER END OF the line: "*Happy Birthday.*" That was spooky--the next day I would turn 37. "Your full name is Adam Landis Penenberg," the caller continued. "Landis?" My mother's maiden name. "I'm touched," he said. Then Daniel Cohn, Web detective, reeled off the rest of my "base identifiers"--my birth date, address in New York, Social Security number. Just two days earlier I had issued Cohn a challenge: Starting with my byline, dig up as much information about me as you can. "That didn't take long," I said.

"It took about five minutes," Cohn said, cackling back in Boca Raton, Fla. "I'll have the rest within a week." And the line went dead.

In all of six days Dan Cohn and his Web detective agency, Docusearch.com, shattered every notion I had about privacy in this country (or whatever remains of it). Using only a keyboard and the phone, he was able to uncover the innermost details of my life--whom I call late at night; how much money I have in the bank; my salary and rent. He even got my unlisted phone numbers, both of them. (End of excerpt)

One might wonder who Dan Cohn is and whom he sells this information to. Forbes

answered that as well:

Cohn operates in this netherworld of private eyes, ex-spooks and ex-cops, retired military men, accountants and research librarians. Now 39, he grew up in the Philadelphia suburb of Bryn Mawr, attended Penn State and joined the Navy in 1980 for a three-year stint. In 1987 Cohn formed his own agency to investigate insurance fraud and set up shop in Florida. "There was no shortage of work," he says. He invented a "video periscope" that could rise up through the roof of a van to record a target's scam.

In 1995 he founded Docusearch with childhood pal Kenneth Zeiss. They fill up to 100 orders a day on the Web, and expect $1 million in business this year. Their clients include lawyers, insurers, private eyes; the Los Angeles Pension Union is a customer, and Citibank's legal recovery department uses Docusearch to find debtors on the run.

Cohn, Zeiss and 13 researchers (6 of them licensed P.I.s) work out of the top floor of a dull, five-story office building in Boca Raton, Fla., sitting in cubicles under a fluorescent glare and taking orders from 9 a.m. to 4 p.m. Their Web site is open 24 hours a day, 365 days a year. You click through it and load up an on-line shopping cart as casually as if you were at Amazon.com. (End of excerpt)

Amazingly, Cohn admits to the use of fraud and bribery:

The researchers use sharp sifting methods, but Cohn also admits to misrepresenting who he is and what he is after. He says the law lets licensed investigators use such tricks as "pretext calling," fooling company employees into divulging customer data over the phone (legal in all but a few states). He even claims to have a government source who provides unpublished numbers for a fee, "and you'll never figure out how he is paid because there's no paper trail." (End of excerpt)

The following excerpt reveals methods used by Cohn directly relevant to today's hearing and HR 4311:

Cohn's first step into my digital domain was to plug my name into the credit bureaus--Transunion, Equifax, Experian. In minutes he had my Social Security number, address and birth date. Credit agencies are supposed to ensure that their subscribers (retailers, auto dealers, banks, mortgage companies) have a legitimate need to check credit.

"We physically visit applicants to make sure they live up to our service agreement," says David Mooney of Equifax, which keeps records on 200 million Americans and shares them with 114,000 clients. He says resellers of the data must do the same. "It's rare that anyone abuses the system." But Cohn says he gets his data from a reseller, and no one has ever checked up on him.

Armed with my credit header, Dan Cohn tapped other sites. A week after my birthday, true to his word, he faxed me a three-page summary of my life. He had pulled up my utility bills, my two unlisted phone numbers and my finances. (End of excerpt)

And should there be any question as to the ability of a determined criminal to gain access to confidential information including financial information, the following excerpt is on point:

He had my latest phone bill ($108) and a list of long distance calls made from home--including late-night fiber-optic dalliances (which soon ended) with a woman who traveled a lot. Cohn also divined the phone numbers of a few of my sources, underground computer hackers who aren't wanted by the police--but probably should be.

Knowing my Social Security number and other personal details helped Cohn get access to a Federal Reserve database that told him where I had deposits. Cohn found accounts I had forgotten long ago: $503 at Apple Bank for Savings in an account held by a long-ago landlord as a security deposit; $7 in a dormant savings account at Chase Manhattan Bank; $1,000 in another Chase account.

A few days later Cohn struck the mother lode. He located my cash management account, opened a few months earlier at Merrill Lynch &Co. That gave him a peek at my balance, direct deposits from work, withdrawals, ATM visits, check numbers with dates and amounts, and the name of my broker. (End of excerpt)

Cohn is even willing to lead officials to believe he is a law enforcement officer as this excerpt demonstrates:

How did Cohn get hold of my Merrill Lynch secrets? Directly from the source. Cohn says he phoned Merrill Lynch and talked to one of 500 employees who can tap into my data. "Hi, I'm Dan Cohn, a licensed state investigator conducting an investigation of an Adam Penenberg," he told the staffer, knowing the words "licensed" and "state" make it sound like he works for law enforcement.

Then he recited my Social Security, birth date and address, "and before I could get out anything more he spat out your account number." Cohn told the helpful worker: "I talked to Penenberg's broker, um, I can't remember his name...."

"Dan Dunn?" the Merrill Lynch guy asked. "Yeah, Dan Dunn," Cohn said. The staffer then read Cohn my complete history--balance, deposits, withdrawals, check numbers and amounts. "You have to talk in the lingo the bank people talk so they don't even know they are being taken," he says. (End of excerpt)

But the Forbes reporter (Penenberg) did some further digging and uncovered what appears to be direct evidence of the use of impersonation and pretext in the following excerpt:

Sprint, my long distance carrier, investigated how my account was breached and found that a Mr. Penenberg had called to inquire about my most recent bill. Cohn says only that he called his government contact. Whoever made the call, "he posed as you and had enough information to convince our customer service representative that he was you," says

Russ R. Robinson, a Sprint spokesman. "We want to make it easy for our customers to do business with us over the phone, so you are darned if you do and darned if you don't."

Bell Atlantic, my local phone company, told me a similar tale, only it was a Mrs. Penenberg who called in on behalf of her husband. I recently attended a conference in Las Vegas but don't remember having tied the knot. (End of excerpt)

Finally, Cohn believes he is justified in what he does:

Daniel Cohn makes no apologies for how he earns a living. He sees himself as a data-robbing Robin Hood. "The problem isn't the amount of information available, it's the fact that until recently only the wealthy could afford it. That's where we come in." (End of excerpt)

I have one question. Why are Dan Cohn and Docusearch still in business?

Docusearch is not alone. There are now more information brokers and private investigators openly advertising their ability to obtain and sell financial information then there were in 1998. These ads continue to be found on the World Wide Web, in the yellow pages and in legal and investigative trade journals. In fact, there has been an ad running in the local edition of the Legal Times that can be found in many law firms and federal offices here in Washington. I suspect copies can be found at the FBI, U.S. Attorney's Office, the Department of Justice, and the Federal Trade Commission.

One phone call to this company determined they offer the ability to locate an address for an individual for $65 if the social security number is provided and $115 if the social security number is not provided. Further, and more to the point, for $200 they will supply the name of the bank, the type of account maintained and the balance in the account for the individual specified. There was a further offer extended by the company to confirm that the funds are available and there would be no charge if there were only minimal funds in the account. The scenario presented to the company fell squarely within the four corners of Gramm-Leach-Bliley that would make the request and provision of the banking information illegal if accomplished by pretext. The company was informed that a woman was trying to locate a current address for a live-in boyfriend who had skipped town with money from her checking account. There was nothing in the scenario presented that even began to come close to the exceptions enacted as part of Gramm-Leach-Bliley.

In fact, as the committee is aware, on August 30th Committee Senior Counsel Jim Clinger, Special Agent John Forbes, Committee Staff Member Alison Watson and I called numerous private investigators and information brokers around the country in an effort to determine how many would sell bank account information and under what circumstances. We decided that we would survey the first ten companies that we could reach by phone. The companies were selected randomly by Special Agent Forbes based upon their advertisements. All of the companies were presented with the scenario outlined above.

In less than three hours the first ten companies we reached were all willing to sell us personal bank account information detailed enough to raise the educated belief that the information would be obtained by pretext or other deceptive means. Not a single company we reached turned us down. Not one.

More to the point, two of the companies' representatives made specific mention of "privacy laws" and "federal statutes" being a hindrance to their ability to provide the information. However, we were told, they could still succeed but just "don't tell anybody" that we had obtained the information.

One individual referred to the fact that he had 11 years banking experience and guaranteed that he could find the bank and that 80% of the time he could get the account number and balance. Several of the companies stated that they could get us individual transaction records including deposit information.

One offered to teach us how to determine the amount in the account once he located the bank and account number.

One company stated that it would check the Federal Reserve section for the part of the country where the individual was located. This same company claimed to work for "hundreds and hundreds of attorneys and collection agencies". Further, they stated that they had found $1.2 million dollars in an account just the previous day for an attorney. They advised us to wait for the banking information before going to Court.

Another company stated they would locate the information if we had a "Court filing judgment" or a letter from an attorney giving the name of the person the account information was being sought for and the reason. This company stated they could find local bank information for $200 and statewide information for $500 including account numbers and balances.

Several of the companies offered to locate safety deposit box locations and securities related information. One company charges $175 to locate the name and address of the bank if you have a judgment. However, the same company offered for $250 to locate all accounts, account numbers, balances, mutual funds, names on the accounts, dates of closure if an account was closed, and safety deposit box information if we didn't have a judgment.

Here is just one example of the type of advertising we found:

Welcome to (name omitted). We can perform bank account and investment searches anywhere in the USA and the World. Bank account searches can be used to collect judgements, verify net worth of individuals and companies, or any other purposes.

We can search:
Bank Accounts
Checking
Savings

Investments
Stocks
Bonds
Commodities
Mutual Funds
Safety deposit boxes
And much, much more...

We can search by:
State
Country
Offshore account searches also available.

Disclaimer: **We limit retrieval to documents or information available from a public entity or public utility which are intended for public use** and do not further elaborate on that information contained in the public entity or public utility records. Must Be 18 or Older for a Consultation or Record Search. We take no responsibility and assume no liability for any privacy claims as **we neither utilize, reveal, nor attempt to access any confidential information concerning the parties involved** in the search. We are not a licensed private investigator, and we do not engage in any activities for which a license is required... (End of excerpts)

The disclaimer is amazing in light of the fact that this company offered to sell us the amount located in a checking account and the deposit history to the account for $275. I cannot fathom a single way that account balance and deposit transaction records could be "intended for public use". Indeed this would be a direct revelation of "confidential information".

No company we reached asked any questions that would logically follow from the passage of Gramm-Leach-Bliley, even when they had disclaimers in the advertisements suggesting that there were restrictions on who could obtain banking information and under what circumstances. Further, in addition to the overt remarks made by several companies to the minor obstacles presented by "federal statutes" and "privacy laws" the advertisements and telephonic presentations bore all the classic signs of pretext operations. These include no-hit/no-fee guarantees; length of time required to complete the search; higher pricing; and types of information being sold.

These results are troubling and point to the inescapable conclusion that there are now criminals hiding behind professional titles such as "information broker", "private investigator", and "judicial judgment collector". I do not make this statement lightly as I was a private investigator for seventeen years and was very proud of my profession. There are thousands of good, honest private investigators, information brokers, and collection professionals working everyday in this country to assist citizens and attorneys at all levels of our judicial system. I receive emails everyday from investigators and brokers who are upset and demoralized because of the practices of some who feel it is easier to steal information instead of using the lawful means that all others who obey the law do. The good, honest professionals are looking to their government to step in and

stop these criminals.

Further, many of the information brokers, private investigators, and judicial judgment collectors belong to national trade associations. In fact, many of these association members and their leaders can be found in Internet chat areas trading pretext methods. This begs the question: What are these associations doing to police their membership?

The Effectiveness Of Efforts By The Financial Services Industry To Deter And Detect Fraudulent Attempts To Obtain Confidential Account Information

The financial services industry has for many years utilized various methods of combating fraud and protecting the confidentiality of customer information. As I stated in my testimony two years ago, I believe the industry was not aware of the techniques being used by information brokers and investigators to penetrate their security protocols by means of pretext and impersonation. Indeed, most Americans remain ignorant of the practices of unscrupulous information brokers. The financial services industry is traditionally between a rock and a hard place when it comes to information security. Customers want their information to remain confidential. At the same time, they want easy access twenty-four hours a day to that same confidential information. It is this very dilemma that criminals exploit.

The financial services industry is starting to move aggressively to combat the methods and deceptive practices used by identity thieves and infobrokers that seek to illegally gain access to confidential information and in many cases to steal the funds of institution customers. Upgraded and newly developed computer systems and programs work to oversee billions of transactions each day in an effort to identify potentially fraudulent activity. Education and training programs are being modified and instituted to teach all institution employees the signs of identity theft and fraud and what steps to take.

Institutions that have taken steps to determine if information brokers are attempting to access confidential information have found that this is indeed the case. More and more institutions are moving to institute passwords and personal identification numbers (PINS) that provide true access protection. But, many more need to move in that direction. Customers are starting to be notified by institutions concerning the reason and need for certain security protocols. Again, more needs to be done in this area. There is much education, training and work that remains. I am convinced the financial services industry is up to the task.

I have had a birds-eye view of the response of the financial services industry over the past two years. I have worked directly with institutions and professional associations to educate them on the issue of pretext and other deceptive practices used to penetrate information security systems. In each instance I have found that the privacy, administrative and security leaders in the institutions and at association meetings are genuinely concerned about solving this problem and are moving to do so. The financial services industry relies on a reputation for confidentiality to survive. Recent well

publicized cases of institutions not protecting customer information both here and abroad illustrate the harm that will quickly be realized by an institution that does not protect customers.

This concern has led, in one instance, to the American Bankers Association distributing to the entire membership an education and basic training program on pretext calling I was asked to author at the association's initiative. The portion I authored was just a small part of a comprehensive three part series the ABA has distributed to the membership to address the subject of identity theft and privacy in detail over the course of this past year. I believe these materials will aid in thwarting the practices of the Dan Cohns of this world.

I have been asked to speak on a number of occasions to groups of bankers to demonstrate to them how to spot pretext calls, how to educate financial services employees about pretext, and what steps to take at the institution level to thwart information security intrusions. Indeed, you would be hard pressed to find a gathering of bankers anywhere today where the subject of privacy is not addressed at length as a major topic of discussion. Further, the financial services industry did not wait for the passage of GLB to address the issue of pretext. Almost immediately after my testimony in 1998 the ABA was distributing materials and videotapes to any institution concerning pretext and updated information security practices.

It is too early to tell how effectively the defenses now being installed by financial institutions are working to thwart pretext. However, judging by the number of firms advertising the ability to obtain financial information there is still more to be done.

However, unless we end legitimate customer access to account information, there will always be criminals who will attempt to steal that information. The financial services industry needs a helping hand from law enforcement. These criminals must be prosecuted. The message needs to be sent that Federal law enforcement is serious about protecting financial institution customers. It is time to act.

Emerging Threats To Financial Privacy

While the traditional methods of pretext presented before this Committee two years ago continue, there are new emerging threats to the security of information within financial institutions. Those who use creative means to obtain personal information are not resting and waiting to see what Congress or law enforcement will do next to protect the privacy and confidentiality of U.S. citizens. These individuals and companies continue to develop methods to locate citizens and their confidential information. There is much fear that the loss of routinely accessed credit headers will diminish the ability to easily access personal biographical information used as part of a pretext. Therefore, some who seek that information are moving to develop other "sources" and "methods" to develop personal information needed to begin a successful pretext.

The fastest growing method used to "skiptrace" for the current address and other

personal information of an individual is to obtain the information from the phone company. Most United States citizens believe that their phone records are private unless obtained by subpoena or other form of Court order. This is especially true for the millions of Americans who pay extra to have a non-published or unlisted phone number. Most citizens would further think that who they call and how long they talk is also a private matter. Most citizens would be wrong.

For years I have seen the sale of private telephone information on the web and in investigative and legal trade journals. These services include the acquisition and sale of non-published and unlisted phone numbers and records; long distance toll records; cellular phone records; pager records; fax records; the current phone number and address for the owner of a disconnected phone, and much more.

While these practices are bad enough, and need to be addressed by Congress and/or law enforcement, the latest development is equally worrisome. Currently, there are presentations of closed, highly secure classes for private investigators and information brokers, teaching the inner workings of the telecommunications industry. These classes are being coupled with databases being developed in the private investigative community to assist in obtaining information held by telecommunications companies. Once obtained this data can then be sold and/or used as part of further identity theft and pretexts used in any number of scenarios, but certainly as the starting point for information gathered as part of a pretext against a financial institution or directly against the financial consumer.

Here is an advertisement being widely distributed for these classes:

NOW! COMING TO LOS ANGELES!
Telecom Secrets Seminar
or
Using Telecom as a new way
to skiptrace and locate.
by
Michele "Ma Bell" Yontef, CMI
Telecom Investigations Specialist, Licensed Private Investigator,
Paralegal, Server of Process, Notary, Constable of Court

****

This is a seminar that will take you from being someone who uses a phone in investigations, to someone who uses the whole telecommunications system to further your investigations. You will gain a comprehensive understanding of the phone system, and how to use that system to get the information you need to close the case. **With so many of our "tools of the trade" being taken from us by recent privacy laws, this is a "must attend" seminar.** Using Michele's completely legal methods we can continue to obtain the information that is vital to us and to our clients. Don't let yourself or your clients down, learn new and better ways to increase your services and your income.

No recording of any kind will be permitted. There will be extensive security measures. Please contact Vicki for details. All attendees will be required to sign a non-disclosure agreement.

West Coast Professional Services reserves the right to refuse admittance.
These techniques are completely legal, but are being taught only to Investigators and Law Enforcement Officers. Restrictions apply.
****
****

A statement from Michele regarding the content:

I will be talking about everything from how to make totally anonymous calls to finding the carrier of any type of line. I will be explaining how things in the Telecom work, so that you will know how to legally maneuver around any obstacle. **I will show you how to skip trace and locate like never before, by using the Telecom as a database.** I will tell you what the operator knows about you, who can hear you talking on the phone, how to perform all types of procedures, and I will be giving you a ton of vital information in my booklets that accompany the seminar. **I will also introduce a new form of searching for skips and will open to you first, my brand new database, that encompasses EVERY numerical search you have ever seen online, plus many more new search ideas that I can teach you about in the seminar as well.** For example, did you know that the type of switching your telephone company has you hooked into can allow a listen in on your lines...I will explain how to tell what kind of switching you have, and how it can either lend to the listen in, or block it. I can also show you how to use my database to find that switching for any party, and use it to trace a number to CNA, without ever picking up the phone to pretext anyone! I have brought home missing children, using the secret searches I will disclose to all of you that attend. (End)(Emphasis added)

Here is another widely distributed reference:

Here's an unedited letter from (name deleted), who just experienced the Telecom Secrets Seminar by Michele "Ma Bell" Yontef...

Colleagues:

There are currently three days to prepare yourself, if you are attending the Los Angeles version of the "Telecom secrets" Seminar. You need to practice taking notes, and be ready to absorb the information like a sponge. There is a lot of it, but it's actually very easy to learn. **Michele teaches you about how the entire telecommunications system works, then gives you the secrets of how you can use it to do your own non-pubs, CNA's and disconnects, as well as the rationale that leads you to be able to determine the location of some of the toughest skiptrace assignments and locates, you have ever attempted.** I sat in awe, writing as furiously as I could, through the six hour session with the Iowa Association of Private Investigators, (IAPI), provided by Michele, on Friday afternoon. I cannot tell you how valuable this seminar will be to me, in the coming weeks and months, as I develop my skills, using her technique. The best part is that I'd never even thought of most of this stuff. It is all new, and a wonderful way to expand one's skiptracing skills. It will take practice, but

she has given us all a true treasure chest, (and she knows how I love treasure chests! --<grin>), and all the other tools to do the job. The price is an absolute bargain, too!

Please pay particular attention to the reason for her disclaimers and nondisclosure forms. **With all the movement and political wrangling of the privacy advocates, (READ - "reactionaries"), we can't afford to have this excellent legal source tainted by the people who would strangle our profession, and shut off all our sources.** End) (Emphasis added)

The reference to "CNA's" means customer name and address. The reference to "non-pubs" means the ability to obtain the non-published phone number for an individual. The reference to "disconnects" means the ability to locate the new phone number, name and address for someone who disconnected a phone in addition to determining the owner of a previously disconnected phone number.

The database being designed to aid in the acquisition of information maintained by the telecommunications industry has been named "The Last Treasure". The choice of this name is intentional. It was chosen to mean that this database will be the last method available to locate the overwhelming majority of citizens should the carte blanche acquisition of credit header information be restricted. As with the pretext of financial institutions two years ago, the presenters of these classes and the developers of this database claim that this is all legal. I will leave that to others to decide. As a citizen of this country I am dismayed that my phone records can be bought and sold on the Internet. As a former private investigator that has handled several stalking cases I am well aware of the damage that can be done through the acquisition and sale of this information. As a privacy consultant, I am well aware of the fact that information obtained from the phone company can and is often used to start a financial pretext.

Should there be any doubt concerning the problems that can be created when confidential phone information is obtained, one look no further then a September 9, 2000 article by Lindsey A. Henry for The Des Moines Register:

A West Des Moines woman contends that her ex-husband tracked her down and threatened her after MCI WorldCom gave out her phone number and other information.

Peggy Hill, 33, is suing the long-distance company in federal court in Des Moines. The lawsuit says her ex-husband in Georgia called MCI at least 10 times in June 1999 asking for her billing information and the numbers she had called.

MCI representatives gave him the information and even changed her calling plan at his request, the lawsuit said. (End of Excerpt)

Here was a woman being stalked by her ex-husband and taking precautions, only to be thwarted by the ease with which her phone records were accessed:

Hill thought she had protected herself, her lawsuit says. She moved several times after her divorce in 1992. She paid for an unlisted number. She asked MCI to keep her information confidential, according to the lawsuit.

Only after Hill called to complain did MCI employees flag her account with a warning, according to subpoenaed MCI files.

"Please do not look up numbers for him or give him names of where numbers are dialed to," the notation said. "Peggy is in danger!!!!!! . . . MCI should not have given this man any information!!!!!!" (End of excerpt)

The following claim of rarity when it comes to the release of confidential phone records is laughable given the ease with which Infobrokers buy and sell phone company customer records every day and widely advertise their ability to do so on the Internet:

Sandy Kearney, an investigator for the Iowa attorney general's office, said Hill's situation was rare.

"I hear all the time from telephone companies claiming to not release information without permission," she said.

Hill's lawyer, George LaMarca, said the lawsuit should remind companies of their obligation to protect customers.

"We can't get services without entrusting our most confidential and personal information to companies," LaMarca said. "When we do that, we expect confidentiality. When that trust is breached, companies should expect to pay the consequences." (End of excerpt)

Just as this husband was able to allegedly access his ex-wife's customer records, identity thieves, private investigators, information brokers and judicial judgment collectors use similar techniques everyday to access these same records. All they need do is impersonate the customer or the relative of a customer. This common knowledge amongst identity criminals is being used as the starting point for access to personally identifiable information that can then be used to access financial information.

This committee will recall the testimony of one of the "Godfathers" of the information broker industry in this very room two years ago. Al Schweitzer instructed us all at that time that one of the most common financial pretexts begins with either a pretext call to the consumer impersonating someone from the phone company, or a pretext call to the phone company to develop personal information to be used as part of a further pretext against the consumer and/or financial institution. The problem continues today and is growing in scope and sophistication.

I would like to ring one final warning bell concerning the use of pretext and deceptive information security penetration practices. These are the very techniques that are used by individuals engaged in corporate espionage. Every day these techniques are used to steal our nation's corporate and military trade secrets and other forms of confidential information. I know that our military is aware of this as representatives of the Pentagon asked me to present a private briefing after my last appearance here in 1998. I will not disclose in an open forum what I was able to demonstrate in that briefing other than to

state that I believe it confirmed concerns on the part of the officials I met with in relation to a threat that could easily put our country at a disadvantage during a time of crisis.

This Committee, which oversees the safety and soundness of our Nation's financial system, should be concerned about the threat that corporate espionage, both domestic and foreign, poses to the financial well being of our country. This is the "Information Age" and our country is the leader in that regard. It is precisely that leadership position which is driving this unprecedented economic boom we are all witnessing. Information technology advantages are paramount to our continued economic success. This is why information security is all-important to that success. Companies are discovering the need for computer system firewalls, yet are woefully unprepared when it comes to social engineering security penetrations and a laissez faire attitude concerning who information is disclosed to telephonically and otherwise.

Simply put. Loose lips do sink the corporate ships of today and tomorrow. The most infamous computer "hacker" on the planet, Kevin Mitnick, obtained the plans for an unreleased Motorola product by direct "pretext" phone calls to Motorola employees who then faxed him the plans to his home! If you speak to Mr. Mitnick, you will learn that he obtained just as much confidential information via "dumpster diving" and social engineering (pretext) as he ever did by a true computer hack attack.

Another method that is becoming more common is the use of a "Trojan check". An investigator or broker will create a fictitious business name and open a checking account in that business name. A small check will be mailed to the target as a "rebate" or "prize" stamped on the back "for deposit only". Once the check has been deposited and is returned to the fictitious company the banking information obtained on the back of the check can be used to further the pretext to determine the amount of funds held in the account. There is great debate in the investigative and broker communities as to the legality of this practice given Gramm-Leach-Bliley and the deceptive trade practices statutes. While the debate continues, so does the practice.

Informal networks of investigators, infobrokers, judgment collectors, and collection professionals are found all over the Internet. It is not uncommon to see requests for "contacts" in financial services institutions. Some collection professionals openly advertise their ability to provide information maintained within their files. Routinely, there are account and file numbers along with the names of targets placed on the Internet for inspection by others to determine if information can be traded or obtained.

Vehicle tracking devices are being offered for sale in order to follow or record the travels of citizens. While not directly relevant to the pretext of financial information, it demonstrates the length that some will go to in order to obtain information on citizens in the United States today.

If law enforcement agencies of State and Federal governments were caught doing these practices absent a constitutionally permissible purpose and/or Court order there would be rioting in the streets. Yet every day these events are carried out by private

investigators, information brokers and judgment collectors who have no authority above that of a private citizen and no one blinks. From where I sit, my privacy is just as violated whether the intrusion comes from a person with a badge or not.

What Needs To Be Done

I would like to make some suggestions concerning what needs to be done to continue the battle against the use of fraud and deception to access financial information.

First, we need swift, aggressive, nationwide action by law enforcement to begin criminal investigation and prosecution of those who are thumbing their noses at the provisions of Gramm-Leach-Bliley and other appropriate statutes. I hope the information I provided in 1998 and today supports this conclusion.

Second, GLB needs to be amended. The narrowly crafted child-support exemption for the use of pretext is being used as an advertising shield by private investigators to hide behind while continuing the covert sale of financial information that falls outside of the GLB exemptions. The provisions of GLB that allow for pretext in a child support situation state as follows:

Sec. 521 (g) NONAPPLICABILITY TO COLLECTION OF CHILD SUPPORT JUDGMENTS- No provision of this section shall be construed to prevent any State-licensed private investigator, or any officer, employee, or agent of such private investigator, from obtaining customer information of a financial institution, to the extent reasonably necessary to collect child support from a person adjudged to have been delinquent in his or her obligations by a Federal or State court, and to the extent that such action by a State-licensed private investigator is not unlawful under any other Federal or State law or regulation, and has been authorized by an order or judgment of a court of competent jurisdiction.

The operative language is: "No provision of this section shall be construed to prevent any State-licensed private investigator…from obtaining customer information of a financial institution...to collect child support from a person adjudged to have been delinquent in his or her obligations by a Federal or State court...**AND** has been authorized by an order or judgment of a court of competent jurisdiction." This language clearly means from both the legislative history of the act and the plain face of the statute that a judge (Court) must specifically authorize the use of pretext to obtain customer information of "a financial institution".

I am not aware of a single case where a Court has authorized a private investigator to intentionally deceive a financial institution in order to obtain customer information. It is easy to understand why this has not happened and most likely never will. The presumptive evidentiary burden that would be required to obtain such an order would easily support the issuance of a subpoena to the institution that the information is being sought from and is being contemplated for pretext. Unless Congress has evidence that financial institutions routinely falsify responses to subpoenas it is hard to fathom why this

provision was placed in GLB.

Further, this section states: "to the extent reasonably necessary to collect child support from a person adjudged to have been delinquent in his or her obligations by a Federal or State court." The legislative history of this exemption was a claim made by some representatives of the private investigative industry that pretext was needed as there was no other method available to locate the financial institution holdings of deadbeat parents who lie to the Courts. This claim was not true at the time, as there are many lawful ways to pursue overdue non-custodial child support payments and many taxpayer funded agencies designed to fill that role. However, even if this argument is accepted as a legitimate historical reason for the exemption, there is no longer any legislatively justifiable reason to maintain the exemption given the provisions of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 which are now in effect and mandate that all financial institutions cooperate with the government by providing the financial information of delinquent child support parents directly to the Federal government for asset forfeiture.

The following excerpt describing this procedure is from a front-page article written by Robert O'Harrow, Jr. in the Sunday, June 27, 1999 edition of the Washington Post:

As part of a new and aggressive effort to track down parents who owe child support, **the federal government has created a vast computerized data-monitoring system that includes all individuals with new jobs and the names, addresses, Social Security numbers and wages of nearly every working adult in the United States.**

Government agencies have long gathered personal information for specific reasons, such as collecting taxes. But **never before have federal officials had the legal authority and technological ability to locate so many Americans found to be delinquent parents** -- or such potential to keep tabs on Americans accused of nothing.

The system was established under a little-known part of the law overhauling welfare three years ago. It calls for **all employers to quickly file reports on every person they hire and, quarterly, the wages of every worker. States regularly must report all people seeking unemployment benefits and all child-support cases**.

Starting next month, the system will reach further. **Large banks and other financial institutions will be obligated to search for data about delinquent parents by name on behalf of the government, providing authorities with details about bank accounts, money-market mutual funds and other holdings of those parents.** State officials, meanwhile, have sharply expanded the use of Social Security numbers. Congress ordered the officials to obtain the nine-digit numbers when issuing licenses -- such as drivers', doctors' and outdoorsmen's -- in order to revoke the licenses of delinquents.

Enforcement officials say the coupling of computer technology with details about individuals' employment and financial holdings will give them an unparalleled ability to identify and locate parents who owe child support and, when necessary, withhold money from their paychecks or freeze their financial assets. (End of excerpt) (Emphasis added by Robert Douglas)

O'Harrow went on to describe in more detail how the new system operates:

Next month, **financial institutions** that operate in multiple states -- such as Crestar Financial Corp., Charles Schwab & Co. and the State Department Federal Credit Union -- **will begin comparing a list of more than 3 million known delinquents against their customer accounts. Under federal law, the institutions are obligated to return the names, Social Security numbers and account details of delinquents they turn up.**

The Administration for Children and Families will then forward that financial information to the appropriate states. For security reasons, spokesman Kharfen said, the agency will not mix the financial data with information about new hires, wages and the like. Bank account information will be deleted after 90 days.

In a test run this spring, Wells Fargo & Co. identified 72,000 customers whom states have identified as delinquents. NationsBank Corp. found 74,000 alleged delinquents in its test.

Later this year, **smaller companies that operate only in one state will be asked to perform a similar service. Officials say most of these institutions will compare their files against the government's. But some operations that don't have enough computing power -- such as small local banks, credit unions and securities firms -- will hand over lists of customers to state officials for inspection. States can then administratively freeze the accounts.**

In California, more than 100 financial institutions have already handed over lists of all their depositors to state officials, including names, Social Security numbers and account balances, a state official said. (End of excerpt) (Emphasis added by Robert Douglas)

Finally, the exemption places GLB in direct conflict with other federal statutes outlawing wire and mail fraud and unfair and deceptive trade practices. The exemption also places GLB in direct conflict with many State laws and creates nothing short of a judicial quagmire.

Simply put, there is no legitimate reason to continue the child support exemption to Gramm-Leach-Bliley. There is a legitimate reason to strike it from the statute as companies are using it as pretence to advertise their ability to locate financial institution customer information. All the ad need say is the request must be in compliance with applicable laws and that all requests are performed on that basis. Once the investigator is comfortable that the requestor is not law enforcement running a sting operation—they sell any information in complete disregard of the law. Our survey proved this ten times over.

Third, financial institutions must continue the work they have started to take every precaution necessary to teach all banking employees about the methods associated with identity theft and pretext so that employees can spot fraudulent acts and know what to do when an act is detected. This will require regular and ongoing education, training and auditing programs to maintain the highest level of information security possible. Infobrokers and identity thieves are constantly developing new techniques and methods. The financial services industry must work to stay abreast of these techniques.

Fourth, the federal regulatory agencies must also continue to stay abreast of information security threats and implement appropriate standards and regulations. Audits need to assess the effectiveness of programs in place.

Finally, this Committee must continue on a regular basis to exercise the appropriate oversight functions necessary to ensure that agencies of the federal government continue to take every step available to stop illegal access of personal and confidential customer information. I know that we are late in the Congressional session and that Chairman Leach will be passing the baton next year. I also am aware that when the baton passes there may be changes in the staff of the Committee. I genuinely hope that no matter who takes up the leadership of the Committee and no matter from which side of the aisle, that there will continue an institutional memory to follow this issue. I truly believe it is of profound import to the health of our financial services industry in this country.

Conclusion

In closing, when I appeared before this Committee in 1998 I recited a long laundry list of the dangers posed by the deceptive methods in use by some private investigators and information brokers to gain illegal access to confidential and protected information. There were some who found it hard to believe that what I claimed was true or as serious as I presented the problem. However, those in the investigative and information broker industries who were practicing these techniques knew that I had spoken honestly and were not pleased to have sunshine illuminating their practices. I soon began fielding phone calls from across the country. The hearing had been carried on C-SPAN. In brief, the attention to these techniques was not well received by some. I was condemned by many and even received two death threats.

I mention this because the information being obtained illegally is in many cases both quite serious and lucrative for those buying and selling it and often places others in physical danger. One needs to look no further than the case of James and Regina Rapp of Touch Tone Services to see that this is true. They were running a million dollar a year operation in Denver Colorado with numerous employees when Denver and Los Angeles law enforcement officers caught up with them along with the FTC. Why so many agencies? A short list of the Rapp's alleged activities points to the answer.

The following allegations were reported: Touch Tone had accessed and sold information concerning undercover Los Angeles police detectives including their private unlisted phone and pager records to a member of the "Israeli mafia", placing the lives of the officers, the officers' families, the officers' confidential informants, and active organized crime investigations in danger. Touchtone accessed and sold information concerning the murder of Ennis Cosby, son of famed comedian Bill Cosby. Touchtone accessed and sold personal and confidential information regarding the Columbine High School massacre victims and families including home addresses, unlisted home telephone numbers, banking, and credit card records.

Touchtone inserted itself into the Jon Benet Ramsey investigation. Here is a list written by James Rapp to a California private investigator outlining the Rapp's work in the Jon Benet Ramsey murder investigation:

Here is a list of all Ramsey cases we have been involved with during the past lifetime (sic).

1. Cellular toll records, both for John & Patsy.

2. Land line tolls for the Michigan and Boulder homes.

3. Tolls on the investigative firm.

4. Tolls and home location on the housekeeper, Mr. & Mrs. Mervin Pugh.

5. Credit card tolls on the following:

a. Mr. John Ramsey, AMX & VISA

b. Mr. John Ramsey Jr., AMX.

6. Home location of ex-wife in Georgia, we have number, address & tolls.

7. Banking investigation on Access Graphics, Mr. Ramsey's company, as well as banking information on Mr. Ramsey personal.

8. We have the name, address & number of Mr. Sawyer & Mr. Smith, who sold the pictures to the Golbe (sic), we also have tolls on their phone.

9. The investigative firm of H. Ellis Armstead, we achieved all their land and cellular lines, as well as cellular tolls, they were the investigative firm assisting the Boulder DA's office, as well as assisting the Ramseys.

10. Detective Bill Palmer, Boulder P.D., we achieved personal address and numbers.

11. The public relations individual "Pat Kroton" (sic) for the Ramseys, we achieved the hotel and call detail where he was staying during his assistance to the Ramseys. We also have his direct cellular phone records.

12. We also achieved the son's John Jr.'s SSN and DOB.

13. During all our credit card cases, we acquired all ticket numbers, flight numbers, dates of flights, departing times and arriving times.

14. Friend of the Ramseys, working with the city of Boulder, Mr. Jay Elowskay, we have his personal info.

Of course, all the above have been repeatedly asked for over and over again.

Let me know if I can be of further assistance in this or any matter. (End of letter)

This one company, Touchtone, had a client list of more than 1,200 spread across the country. Another local Montgomery County, Maryland private investigator admitted to obtaining the phone records of Kathleen Willey, a witness in the criminal investigation of President Clinton. These are just two companies. There are dozens of companies still in operation today. There can be little doubt as to the serious implications of the activities of these companies.

Mr. Chairman and members of the Committee, as I leave you today, I hope that the time and effort I have placed in this testimony will serve as a blueprint for further examination by this Congress of matters deserving attention. Thank you.

"Summary of Senate Finance Committee
Interview of Youssef Hmimssa"
(To be entered into the official record of the U.S. Senate Committee on Finance
in lieu of opening statement by Youssef Hmimssa)

Hmimssa, a 38-year-old Moroccan, arrived in the United States at O'Hare International Airport in Chicago in August of 1994. He traveled from Romania, where he had bought a fraudulent French passport with the alias of Patrick Vuillaume. Hmimssa, who speaks French, said he fit the profile of a North African citizen of France. He simply paid $700 and provided a picture for the fraudulent passport. At O'Hare, he provided his fraudulent passport, where Customs officials stamped it without giving it serious scrutiny.

His original plan was to continue to go to Canada by bus or train and relocate to Montreal, because of his French language skills and because he could not speak English. However, on the flight to Chicago, he met an acquaintance from Romania who told him of the advantages of living in the United States. Hmimssa decided to stay. The acquaintance had a friend drop Hmimssa off in an Arabic neighborhood in Chicago, where he met a Jordanian who needed a roommate. They lived together for about six months.

Hmimssa got a job at a sandwich shop. He needed a bank account, Social Security number and drivers' license so he would not have to take lengthy bus trips to and from work everyday.

He went to a Social Security Administration office and showed his passport, answered a few questions, and a few weeks later received a valid Social Security number and card in the mail. The number was a "non-work" number and appropriately noted on the face of the card.

Soon after that, he went to an Illinois Secretary of State office, which issues driver's licenses. He passed the driving test, and he used a translator to take and pass the written test. He showed his passport, Social Security card, and an envelope he received from Romania at his address. He subsequently received a genuine Illinois drivers' license in the name Patrick Vuillaume.

He wanted to learn English faster so he moved out of the Arabic neighborhood and into the north side of the city where he was forced to use English. He rented an apartment and attended classes for two weeks to earn his taxi driving permit before taking and passing the exam. He was required to pay $500 and have his fingerprints taken and sent to the FBI for a criminal record check.

As he was taking English-language courses, he realized he could not visit Morocco and then return to the United States because his 90 day tourist status, under the name Patrick Vuillaume, was expired. If he was not detained in Morocco, he certainly would not be granted entry back into the U.S.

His goal was to become a United States citizen. He learned that if he obtained a birth certificate and Social Security number, he could then get a valid U.S. passport.

In that pursuit, he paid $700 for what he believed to be a genuine birth certificate and genuine

Social Security card under the name of Edgardo Colon, a U. S. citizen from Puerto Rico. He used those documents to get an Illinois drivers' license, and then applied for a passport at a post office.

He used the Edgardo Colon documents - and a letter he mailed to his own address to the attention of Edgardo Colon - to apply for an Illinois driver's license. At the Secretary of State office, the clerk informed Hmimssa that he already had identification card, and informed him the license was suspended because of overdue fines and traffic violations. She asked several personal questions in an apparent attempt to verify his identity. At this time he spoke limited English and no Spanish. Through sheer luck his answers satisfied her, because she gave him an identification card and told him he could get the license once the $500 fine was paid. Hmimssa paid the $500 fine and went to eight hours of traffic school and received a genuine Illinois drivers' license in the name Edgardo Colon.

At this point, he was driving a taxi cab, renting an apartment, paying his bills and accumulating a good credit rating under the name Patrick Vuillaume. He planned to permanently become Edgardo Colon, a United States citizen. He actually used the Colon U. S. passport to travel to and from Morocco where he spent the 20 days allowed without a visa.

Using the alias Patrick Vuillaume, he applied for and received a credit card under the name Edgardo Colon, claiming that Colon was his roommate.

A short time after returning from Morocco he received a letter from the Internal Revenue Service informing him that the Colon Social Security number was being used by another person. He called the IRS and was asked a number of questions. He then called the Social Security Administration about the Colon number; he was told that there was a recent request for a replacement card. He then realized he had been scammed, and the person who sold him the Edgardo Colon alias had been selling it to others too. Hmimssa decided the Colon alias was now too dangerous to use, so he put it in a safety deposit box for future travel use only.

He then dropped out of college where he had been enrolled under the name Edgardo Colon. He then enrolled in another college to learn computer engineering and become certified with Microsoft programs under the name Patrick Vuillaume.

Using his own personal computer, he surfed the Internet and studied Web sites about how to commit credit card fraud with magnetic encoder reading devices (more commonly known as a skimming device or a "wedge"). Hmimssa also studied computer hacker Web sites where participants trade tips on how to commit computer crimes and other forms of fraud. Although he learned enough that he thought he could create fake identification papers, he did not do so at this time. He started a small business repairing computers and setting up networks, earning about $500 to $700 a week.

He received several job offers from large computer companies, but he had to decline them because he was in violation of his immigration status and he knew they would check with the Social Security Administration and possibly the Immigration and Naturalization Service.

Later, he located a company that employs independent contractors and avoided checking with the Social Security Administration. This job did not work out, so he resumed driving a taxi cab and was deeply in debt. A short time later, he was involved with a dispute with a customer, who filed a complaint against him. A judge revoked his taxi cab license. He continued to drive a cab, often sleeping in his car at the airport.

At this point, he decided to begin committing credit card fraud. When customers would pay him with a credit card, he would swipe it through a skimming device hidden under the front seat of his taxicab.

Using a laptop and basic software, he installed the skimmed (stolen) encoded information onto the magnetic stripe on the back of his Patrick Vuillaume credit card. He began using the false credit card numbers to purchase gas and groceries. Later, he bought computers and other electronics, and then sold the goods at half price. Clerks did not notice that the numbers did not match. A few asked for a driver's license, which he provided, and this matched the name of Patrick Vuillaume on his credit card.

At this point, Hmimssa was earning a lot of money, was paying off his bills, meeting his rent and accumulating a savings account.

Eventually, the scheme came to a stop. His credit card under the name Patrick Vuillaume was declined at an electronics store, and he mistakenly provided a credit card under his other alias, Edgardo Colon. When he provided the clerk with the driver's license under the name Patrick Vuillaume, she figured out the scheme. He grabbed back his license and fled the store. He stopped buying electronics with false credit card numbers for a period of time, but eventually picked a store far outside the city in Rockford, Ill. His credit card was accepted, and when he was asked for his license, he refused. He observed several employees and managers took notice of him, and he figured his description has been distributed to this store.

He fled the store and left his car, which the police eventually towed. Realizing he was being sought by law enforcement, he moved his belongings into storage and moved in with a friend. He began searching for a new alias, and found a Romanian who sold him a Romanian passport, a Social Security card and a sealed envelope from the Social Security Administration for $1,900.

He was subsequently arrested by the Secret Service and released on bond. He later fled Chicago and chose to go to Detroit because of the large Arab population in nearby Dearborn. When he boarded the bus, he provided a new alias, "Jalali." On the bus, he met another Muslim, who helped him get to a mosque when they arrived in Detroit. Hmimssa spent the night there.

The next day he met Ahmed Hannan and Karim Koubriti at a restaurant in Dearborn. He moved in with them and they began to try and recruit him and have him make false identification papers, including drivers' licenses.

Hmimssa and the group often disagreed on political views. The group hated America and Western society; Hmimssa told them he liked American and wanted to make money and take

advantage of the capitalist system. The group said he has been brainwashed by American and Western culture and that he hard forgotten his "people." They often mentioned the conflict between the Palestinians and Israelis. They also expressed their belief that the United States was controlling the Arab world, and how mad they were that the blink sheik was in prison. They also discussed jihad in Chechnya and Algeria. They became skeptical of Hmimssa because he did not share their beliefs. He was never really made a full member of the group because of his disagreements with them.

The Detroit cell members told Hmimssa they wanted to recruit more people to join their group within the country, and to bring in fellow jihad members from overseas. They wanted him to make fraudulent document papers for these overseas persons.

They were particularly angry about Las Vegas, which they called the city of Satan. They were mad that Arabs spent money, consumed alcohol and consorted with women in Las Vegas. They wanted to destroy the city, but they did not discuss specific plans or specific targets.

Hmimssa resisted making fraudulent documents for them and did not do so. As the relationship worsened, he slowly began moving his belongings out of the apartment, one bag at a time, into a nearby apartment. Eventually conflict with the Detroit group erupted, and the men broke into his apartment and stole many of his fraudulent documents. He then went to Chicago and got a new fraudulent green card and Social Security card. He bought a new computer and scanner.

He began working with an individual he knew only as Abdella (real name was Abdel-Ilah Elmardoudi), an associate of the Detroit group who lived in Chicago. He believed he was working only with Abdullah and not the group in Detroit.

Abdella told Hmimssa that security at the Detroit airport was tight, but security at O'Hare was lax, which is why Abdella stayed in Chicago. They wanted him to make fake identification as an FBI agent and as an airport employee, but he declined.

Abdella began bringing "I-94" forms and visas to Hmimssa for him to make fraudulent identity papers. Using a computer scanner, he created blueprints for foreign passports, especially French and Moroccan, and would simply plug in the name and other biographical data.

As part of one scheme to help foreigners enter this country, people would send their picture and information to Hmimssa by fax. He would make a visa and mail it back for the person to put in a passport. The foreigner would then exploit travel agents, who conducted only a cursory, visual check of the passport before issuing an airplane ticket. On the flight to the United States, they would destroy the fraudulent passport and file for refugee or asylum status.

Abdella then helped him move to Cedar Rapids, Iowa, where Hmimssa continued to make false documents. He experimented with making drivers license, but he would not use them himself. He specialized in passports, visas, related immigration documents and other documents that would not likely be subjected to a computer records check. A counterfeit driver's license could result in big problems if subjected to a police records check.

In Cedar Rapids, when he was manufacturing a large number of documents for Abdella (real name Abdel-Ilah Elmardoudi) he used the following method. He would scan passports into his computer and erase the information to make a blueprint. Then he would fill in the information, create a visa, insert a photo, print as a label and place it inside the passport. He used the same blueprint method on "I-94" INS forms - create the blueprint, print it, fill in the biographical information by hand, and stamp it with store-bought stamps. He would then use these documents to obtain Social Security numbers. He would then use both to obtain a written drivers' license.

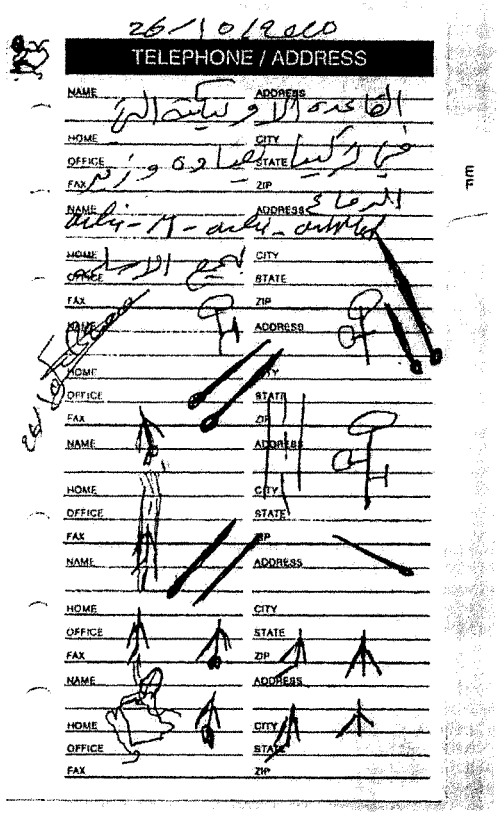
After the attacks of September 11, 2001, he was told to destroy all this papers, but he put them in a storage locker instead.

FBI agents raided his former apartment where Koubriti and Hannan lived and began searching for Hmimssa.

Secret Service agents and Cedar Rapids police caught up with him and arrested him near his apartment on September 28, 2001.

THE RIGHTEOUS SWORD – IN ANSWER TO THOSE WHO CLAIM THAT GOD IS A TYRANT

- Allah, take away the Jews and Christians, and whoever helped them and stood with them.
- Oh Allah, take your enemy, the enemy of religion, that prevented your religion and provoked your religious instructions. Oh Allah, take them away.
- Oh Allah, kill them all and don't keep any of them alive.
- Oh Allah, be without them and whoever believed with them.
- Oh Allah, destroy them with total destruction.
- Oh Allah, tear them apart and divide their gatherings and destroy their unity.
- Oh Allah, praise Islam and the Muslims and provoke the unbelievers and atheists.
- Destroy the enemy of religion.
- Oh Allah, help us with victory and let us be victorious with your soldiers. For you are able to do anything.



LAW ENFORCEMENT SENSITIVE // ORCON

26 Oct 2000

American base in Turkey under command of Defense Minister. For all weapons.

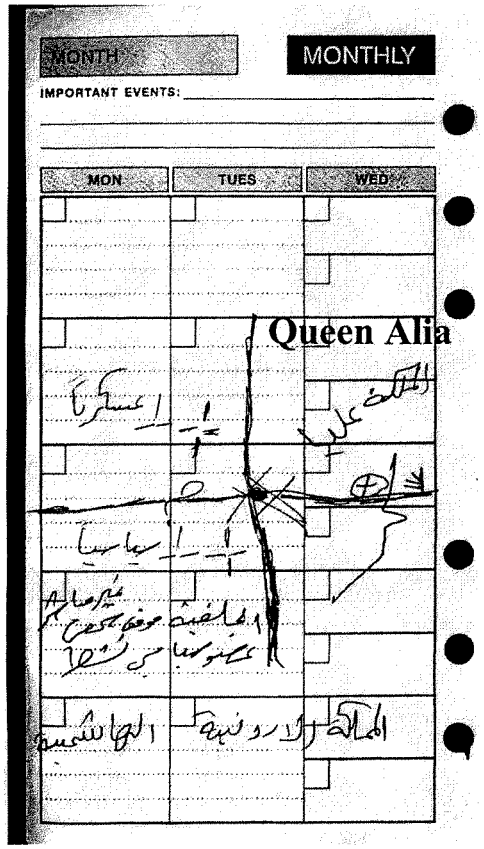
Incirlik Air Base is the only U.S. Air Base in Turkey and is home to Operation NORTHERN WATCH; a coalition force of United States, Turkey, and Great Britain. ONW is responsible for enforcing the "no-fly zone" over Northern Iraq.

GOVERNMENT EXHIBIT 2a27(b)(1)

Factories believed used as surveillance point outside Incirlik AB.
GOVERNMENT

MONTHLY
YEAR
THURS
FRI
SAT/SUN
MONTHLY
YEAR
THURS
FRI
SAT/SUN

Government Exhibit 2A6A



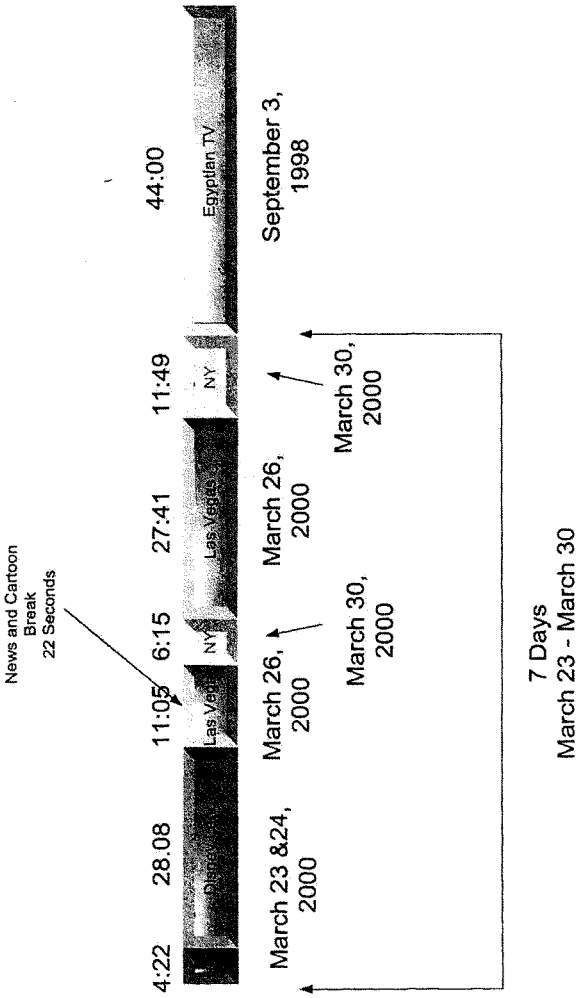
Military

Political

Behind back parking, Private non-direct

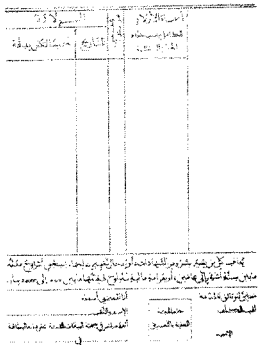
Active Political member

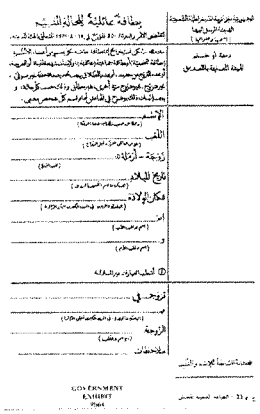
The Hashemite Kingdom of Jordan

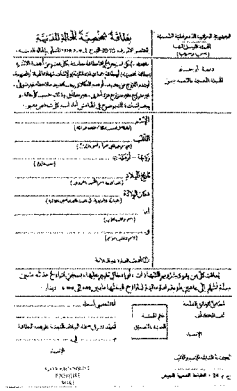

4:22
28.08
11:05
6:15
27:41
11:49
44:00
Diana
Las Vegas
NY
Las Vegas
NY
Egyptian TV
News and Cartoon Break 22 Seconds
March 23 &24, 2000
March 26, 2000
March 30, 2000
March 26, 2000
March 30, 2000
September 3, 1998
7 Days
March 23 - March 30 2000

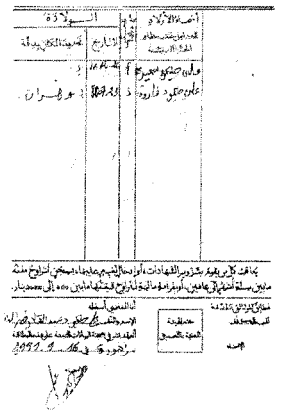
Corroboration of Youssef Hmimssa

- **Hmimssa testified that Ali-Haimoud had access to blank foreign birth certificates. Hmimssa also testified that he did not see any blank foreign birth certificates in the possession of Koubriti, Hannan or Ali-Haimoud. Hmimssa testified that he did not know what country the blank foreign birth certificates were from.**



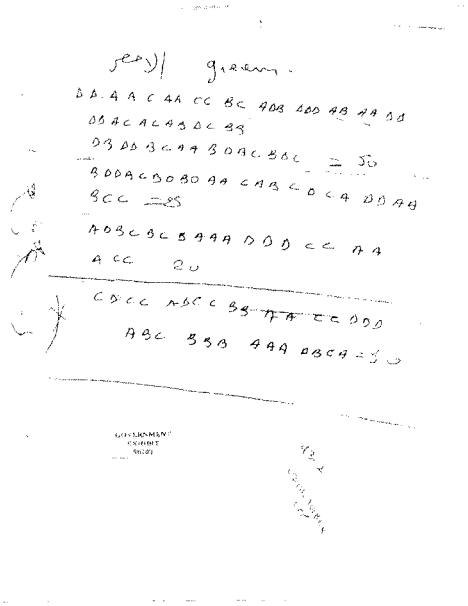


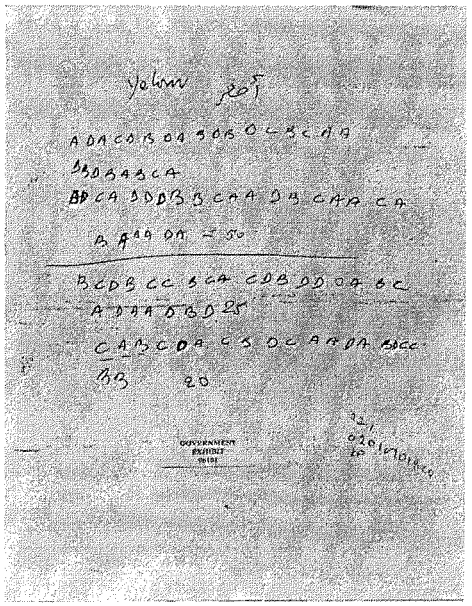




Corroboration of Youssef Hmimssa

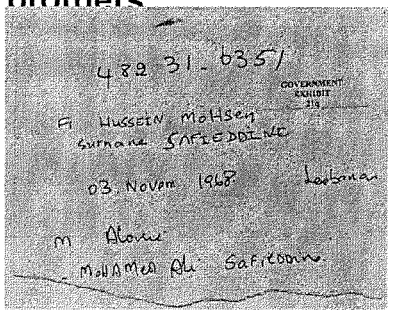
- Hmimssa testified that the Defendants wanted to get a CDL license and haul hazardous materials.

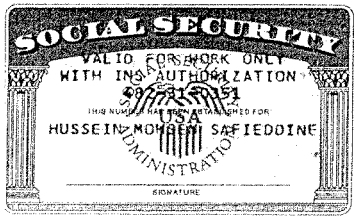


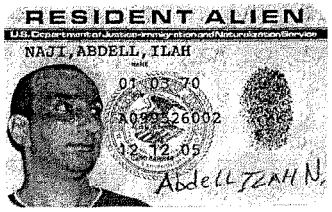


Corroboration of Youssef Hmimssa

- Hmimssa testified that Elmardoudi told him that he had traveled to a city in south Turkey close to the Syrian border called Antakya. Hmimssa testified that Elmardoudi told him that he had traveled there to meet with "brothers."

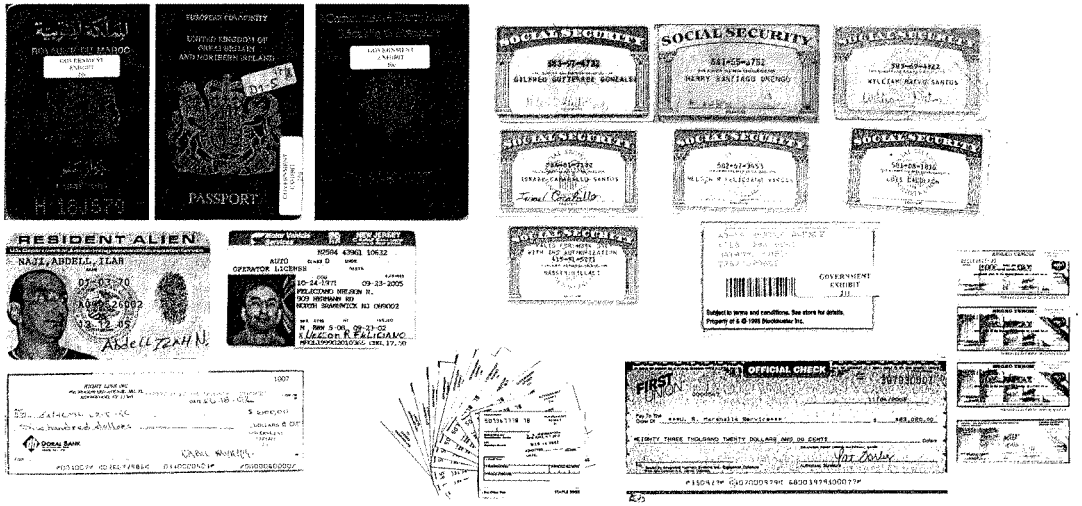






Corroboration of Youssef Hmimssa

- Hmimssa testified that he received foreign passports for alteration from Elmardoudi.
- At the time of Elmardoudi's arrest on 11/04/02, he had in his possession 3 foreign passports, multiple identity documents, 12 blank Immigration I-94 cards, business incorporation documents and stock certificates, a computer scanner, and almost $90,000 in cash and money orders.



TESTIMONY OF ASA HUTCHINSON
UNDER SECRETARY
DEPARTMENT OF HOMELAND SECURITY
DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY
BEFORE THE SENATE COMMITTEE ON FINANCE
SEPTEMBER 9, 2003

Chairman Grassley, Ranking Member Baucus, and other distinguished members, I am pleased to be here today to testify about homeland security and the potential threat of terrorism presented by document fraud, identity theft, and the misuse of Social Security Numbers.

As you know from Congressional hearings, GAO investigations, and press reports, it is certainly possible today to produce or acquire false documents and gain entry into the United States. The Department of Homeland Security and the Directorate of Border and Transportation Security are working actively to address this problem in a number of ways, as I will detail in my testimony.

Despite all these good efforts, we, and the Congress, must be realistic about the results to expect. While we can, over time, reduce the instances when false or fraudulent documents are used to enter the U.S. or to obtain some governmental benefit, there is no easy fix available, and this is a long-term issue for the Congress, the Administration, and DHS to work through together.

DHS is working diligently on all these issues, and my staff has had several meetings with the Social Security Administration to discuss issues of mutual concern and potential ways to reduce the instances where Social Security Numbers are misused.

Description of the Problem

Document Fraud

Fraudulent documents, and, equally as important for the purposes of this hearing and our enforcement efforts, legitimate documents issued as a result of the use of fraudulent "breeder" documents can and are likely used to gain entry into the U.S. and to obtain federal and state governmental benefits each and every day.

As a general rule, the Immigration and Nationality Act requires all U.S. citizens to present a valid U.S. passport to enter or leave the U.S. There are several exceptions to this general rule. The most important applies to travel to and from the U.S. involving "any country, territory, or island adjacent [to the U.S.] in North, South, or Central America excluding Cuba." Thus, as a matter of law, U.S. citizens do not typically need to present a single document -- a passport -- to reenter the U.S. for any travel in the Western Hemisphere.

As a U.S. citizen is not required to present a passport for reentry, federal regulations do not detail what is necessary to validate a person's claim to citizenship in a manner equivalent to that of a passport.

The law requires that a person claiming to be a U.S. citizen "must establish that fact to the examining officer's satisfaction." [8 C.F.R. 235.1(b).]

In operational practice, our inspectors from the Bureau of Customs and Border Protection (CBP) examine any document that may establish identity and place of birth, such as a U.S. birth certificate, driver's license, or whatever else the person's basis for claiming citizenship might be, including baptismal certificates, Certificate of Naturalization, Report of Birth Abroad of U.S. Citizen, or Certificate of Citizenship.

No law or regulation prevents an oral claim of U.S. citizenship in these circumstances. An inspector may, and often does, ask for documentation to support a claim, but this is not currently required. Thus, even if an individual lacks any documentary identification or, as in the case of the GAO investigators who will testify later, the person presents counterfeit documents, inspectors must let the individual back into the U.S. if the inspector is satisfied that the individual really is a U.S. citizen.

By law and practice, CBP inspectors cannot focus their detection efforts on a single document, the passport, and concentrate their expertise on recognizing and blocking the fraudulent use of this one document. As other witnesses have testified before Congress, there are more than 240 different types of valid driver's licenses issued within the United States, and more than 50,000 different versions of birth certificates issued by U.S. States, counties, and municipalities.

Even excluding baptismal records, it would not be easy for CBP inspectors to have a passing familiarity with, let alone a working knowledge of, each of these documents. While advances in technology allow our dedicated and hardworking CBP inspectors to examine and validate documents presented for reentry, that same technology also enables the perpetrators of fraud to produce, relatively inexpensively, high-quality fraudulent documents. Forgers and counterfeiters can produce high-quality fake birth certificates and driver's licenses with off-the-shelf software programs and materials that are difficult to detect without sensitive instruments and sufficient time to examine them.

Our inspectors are also charged with detecting look-a-likes or impostors who attempt to use valid documents which belong to another person. This is one of the fastest growing phenomena in travel document abuse. Document vendors solicit genuine, unaltered documents and match them up with "look-a-likes." The Bureau of Immigration and Customs Enforcement (ICE) has developed a training program to detect impostors, which it has conducted for both U.S. and foreign immigration and border officers around the world.

Equipment costs money, and taking the time to examine thoroughly and in-depth every one of the approximately 460 million identity documents presented at our over 300 land, sea, and air ports of entry would be an enormous undertaking with potentially serious secondary effects. And, even were we to do this, this effort would only permit us to detect fraudulent documents, not, as I will discuss now, legitimately issued documents that are based on identity theft.

Identity Theft

Identity crime is the theft or misuse of an individual's personal or financial identifiers in order to facilitate other criminal activity or to gain something of value. Types of identity crime include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud, and passport/visa fraud. Identity crimes are frequently associated with other crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud, and terrorism.

The topic of identity theft is intimately connected with document fraud. As the GAO and others have shown, it is quite easy today either to obtain or produce on your home computer fraudulent identification documents, such as a driver's license or birth certificate, or to obtain valid documents issued by the appropriate authority (again, driver's licenses, social security cards, etc.) on the basis of false or fraudulent information. For example, it would be relatively easy for an individual to obtain a properly-issued State driver's license in the name of Asa Hutchinson if the individual could establish on the basis of false documents that their name was Asa Hutchinson.

Advances in technology and the explosion of e-commerce have produced enormous advantages for people around the world, and have also conferred benefits on criminals. Information collection has become a common byproduct of e-commerce transactions. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders and include both domestic and international organized criminal groups, street gangs, convicted felons, and terrorists.

The personal identifiers most often sought by criminals are those generally required to obtain goods and services on credit. These are primarily social security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers and personal identification numbers.

Many identity thieves use information obtained from company databases and web sites. One case investigated by the United States Secret Service, the primary DHS agency with jurisdiction over ID theft matters, involved an identity criminal accessing public documents to obtain the social security numbers of military officers. In some cases, the

information obtained is in the public domain while in others it is proprietary and is obtained by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a financial institution, medical office, or government agency.

Just last week, for example, the U.S. Attorney's Office in the Eastern District of Virginia indicted two senior partners of the Fairfax, Virginia law firm Lee & Baker who are alleged to have filed over 50 fraudulent labor certificates for Korean immigrants, who used the bogus documents to obtain green cards to remain illegally in the United States. The arrests and indictments culminated a two-year undercover investigation by federal and local authorities. For those who mistakenly believe that this type of crime does not pay, the immigrants paid $10,000 to $50,000 to obtain the fraudulent employment certifications that were filed with the Labor Departments in Virginia and Maryland.

Identity crime affects all types of Americans, regardless of age, gender, national origin, or race. Victims include restaurant workers, telephone repair technicians and police officers, to corporate and government executives, celebrities and high-ranking military officers.

Of course, and of most relevance to this hearing, fraudulent "breeder" documents obtained through identity theft can then be used to obtain genuine documents from Departments of Motor Vehicles, the Social Security Administration, and elsewhere. These legitimately issued documents can –and are – subsequently used to obtain government services and benefits and to gain reentry into the United States. There is no technology available to CBP inspectors – and none that I am aware of that exists anywhere – that would enable an inspector to determine that a legitimately issued document was actually based on a false breeder document presented to another government agency.

How DHS is Addressing the Problem

DHS and BTS are actively addressing these issues to make it harder for individuals – especially terrorists – to slip into the U.S. using fraudulent documents and to pursue identity thieves and those who use false breeder documents. We also vigorously investigate cases involving the use of fraudulent documents and cooperate with other federal, state, and local governmental entities, as well as the private sector, to heighten awareness and to reduce our vulnerabilities.

DHS uses a combination of advance information about individuals entering the U.S., pre-screening, registration systems such as the US-VISIT and National Security Entry-Exit Registration System (NSEERS), and advanced technology, including the use of biometric information that will be incorporated into our US VISIT entry-exit system.

One Face at the Border

Training CBP inspectors to recognize fraudulent documents is another important step, and one that BTS takes very seriously.

Just one week ago, Secretary Ridge announced that DHS will unify the border inspection process under one Customs and Border Protection Officer, an officer cross-trained to address immigration, customs, and agricultural inspection needs. We will have one face in one uniform -- a single officer trained for primary inspection as well as how to determine who needs to go through secondary inspections.

And since we know that Al Qaeda is interested in entering our ports illegally, this officer -- now trained in all three areas of inspection and armed with the best intelligence we have -- improves our ability to spot and stop terrorists quickly and keep them out. We have already recruited our first group of CBP officers, who will be trained throughout this fall. For DHS, this is another significant step toward our efforts to retool where it makes sense and create efficiencies and unity around a single mission.

All CBP inspectors will receive our most current training on identifying fraudulent and altered documents. CBP secondary inspectors will receive more advanced training, and BTS will continue to maintain the world-class excellence of the ICE Forensic Document Lab (FDL), that was previously housed at the INS.

ICE Resources

The sole mission of the FDL, a fully-accredited crime laboratory, is to detect and deter domestic and international travel and identity document fraud, and the FDL has developed an unparalleled expertise in the area of domestic and international travel and identity fraud.

The ICE FDL maintains a collection of exemplar documents, including birth certificates, passports, and driver's licenses to differentiate valid documents from fraudulent ones. The FDL provides real-time assistance to field personnel in identifying fraudulent documents, produces and broadly distributes Document Intelligence Alerts (high quality photographic bulletins), develops and presents training programs in the detection of fraudulent documents, and works with other Federal, state, local agencies, and foreign governments to promote common efforts to combat international document fraud.

I have brought two samples of these ICE FDL alerts and I commend them to the Members of this Committee. These alerts present, in a clear and simple format, particular features to look for in order to determine whether particular types of documents are fraudulent or counterfeit.

One alert discusses stolen blank Philippine Passports and the other concerns counterfeit Iraqi "N" series passports that were available for purchase in Turkey for about $500. The

alerts highlight how to distinguish immediately between the genuine and counterfeit document.

The FDL has on file intelligence reports of over 100,000 stolen blank, genuine, passports. These passports pose a serious potential threat to national security since they are genuine documents. The FDL has developed a reference guide that contains very precise information on the issuance process of passports and country specific intelligence information. The guide is extremely useful in identifying individuals in possession of these stolen passports.

ICE also operates a Law Enforcement Support Center in Vermont to assist state and local law enforcement officers who have questions about identification assessments during traffic stops. In addition, ICE operates units to link enforcement and intelligence resources with adjudication officers from BCIS who must make determinations about documents that they are presented for adjudication.

In addition to the work of the FDL, ICE law enforcement agents investigate cases of documents and benefits fraud. ICE has joined the U.S. Attorney's Office in the Eastern District of Virginia in a pilot project to investigate and prosecute large immigration, visa, and identification document frauds. The task force includes the participation of the FBI, Social Security Administration, IRS-Criminal Investigation, Department of State, Department of Labor, U.S. Postal Inspection Service, Virginia DMV, and the Fairfax County Police Department.

ICE investigators have logged hundreds of thousands of hours working on counterfeit document related investigations. The primary focus of these cases is to deter, disrupt, and dismantle major criminal enterprises operating not only in the United States, but in source and transit countries as well. The cases often entail long-term, complex investigations that frequently involve our international partners.

Operation Card Shark

I would also like to share the preliminary results of ICE's ongoing investigation, here in Washington, D.C., known as *Operation Card Shark*. *Card Shark* focuses on the street sale of counterfeit documents in the Adams Morgan area. Although the investigation continues, four document mills have already been closed resulting in the seizure of close to 2,000 documents with an estimated total street value of $155,000. 50 aliens have been taken into custody – 30 have been removed from the U.S. and 15 have been prosecuted.

On July 15th, one of the primary targets of this operation was sentenced in U.S. District Court to a total of 52 months in prison for his role as a kingpin in the counterfeit document-manufacturing ring.

Card Shark has disrupted the activity of three significant organizations that operate on the North side of Columbia Road and the return of Pigeon Park to the residents of Adams Morgan.

I look forward to sharing more such successes with you in the months ahead.

US-VISIT

US-VISIT is a crucial new border security and enforcement tool that will capture point of Entry and Exit information by visitors to the United States. This system will be capable of using information, coupled with biometric identifiers, such as photographs and fingerprints - to create an electronic check-in/check-out system for people who come to the United States to work or to study or visit. US-VISIT will also provide a useful tool to law enforcement to find those visitors who overstay or otherwise violate the terms of their visas and will allow us to lock-in an individual's identity, what those in the field call "positive identification" when the individual registers with US-VISIT.

By January 1, 2004, when a foreign visitor flies into one of our international airports or arrives at a U.S. seaport, the visitor's travel documents will be scanned.

Through US-VISIT, all border officers at air and some sea ports of entry will have the capability to access and review the visa information, including the photograph, during a visa holder's entry into the United States. This will enable the border officers to verify the visa photograph with the passport photograph and the individual of the visa holder during their inspection for entry into the United States. Additionally, border officers will capture biometric data to verify and lock-in a visa holder's identity. The US-VISIT system will compare the captured fingerprint against a fingerprint watch list. This will be an enhancement to the existing name check or biographical lookout check.

Prior to departure, the visa holder will have their identity verified at a self-service departure station located at air or seaports. This tells the Department of Homeland Security if that person entered legally or may have stayed illegally as some of the 9/11 terrorists did. Currently, there is no way to know when or even if our visitors leave - but under US VISIT, that will change.

On any subsequent trip to the United States, the visa holder will have their identity confirmed upon arrival and departure. Therefore, the US-VISIT program will have the capability to capture biometrics, confirm the identity of travelers, and search against both a biographical and biometric watch list to prevent document fraud, identity theft, and unauthorized travelers from entering the United States.

All of this information will become part of a foreign visitor's ongoing travel record, so their correct information can follow them wherever they go. The information will be made available to inspectors, agents, consular officials and others with a true need to know.

Mr. Chairman, we should all be clear on my next point. Good information does not threaten immigration. Quite the contrary. The more certain we are about someone's

status, the less likely we are to make a mistake that would jeopardize their status - or our safety.

NSEERS

The NSEERS program requires certain nonimmigrant aliens from designated countries to be fingerprinted, interviewed, and photographed by CBP at our ports of entry at the time they are applying for admission to the United States. In addition, other aliens who are identified from intelligence sources or who match certain pre-existing criteria determined by the Attorney General or Secretary of State may also be enrolled in NSEERS.

NSEERS helps to secure our borders, by intercepting terrorists and criminals at our ports of entry, identifying aliens who deviate from their stated purposes once they enter the U.S., and identifying aliens who have overstayed their visas and are in the country illegally. DHS officers have made every effort to minimize the inconvenience for those individuals required to register, with an average processing time of just 18 minutes.

The NSEERS registration process enables DHS to verify that an alien is living where he said he would live, and doing what he said he would do while in the United States, and to ensure that he is not violating our immigration laws.

During the enrollment process, specific biographic information, itineraries and addresses are collected. If aliens remain in the U.S. for longer than 30 days, they must return to a DHS office to confirm their address and activities in the United States. Registrants must also complete a departure check when they leave the country.

CBP Data Bases

CBP has developed the Image Storage Retrieval System (ISRS), a web based system that provides users at over 40 ports of entry with access to the biographical image sets (photographs, fingerprints and signature) used to create government issued identity documents issued by DHS. These include Alien Registration Cards (I-551s), Employment Authorization Documents), Advance Parole for Adjustment of Status forms issued by BCIS Service Centers, and Refugee travel documents. This tool allows for immediate identity verification resulting in the detection of possible fraud while facilitating the inspection of the legitimate traveler. DHS hopes to roll-out this system to all ports of entry in the next fiscal year.

Identity Theft

DHS is also working hard to reduce the incidence of identity theft, and the Secret Service is leading this effort on behalf of the Department.

This summer, the Secret Service developed and distributed to state and local law enforcement agencies throughout the United States an Identity Crime Video/CD-ROM. The CD-ROM I am holding contains over 50 investigative and victim assistance

resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM contains a short video that can be shown to police officers at their roll call meetings and discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police.

The Secret Service has authorized law enforcement agencies to make as many copies of the CD-ROM as they wish so that the agencies can distribute this resource to their officers to use in identity crime investigations.

The Secret Service is also training state and local law enforcement agencies to prevent identity theft the old fashioned way. In a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police, the Secret Service has hosted Identity Crime training seminars for law enforcement officers in New York, Chicago, Seattle, Dallas, Las Vegas, Washington D.C., Phoenix, Richmond, and Iowa, Mr. Chairman. The Secret Service has additional seminars planned for San Antonio, Texas next month, Orlando, Florida in November, and San Diego, California. These training seminars focus on providing local and state law enforcement officers with tools and resources that they can immediately put to use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

Collaboration

DHS and BTS are also collaborating with others in both the government and in the private sector to combat and address these important issues. We have worked closely with the Department of State on visa issuance issues and obtaining access to the Consolidated Consular Database. My staff has met several times with representatives of the Social Security Administration (SSA) to discuss issues of mutual concern and to explore how to reduce the instances of the misuse of social security numbers.

ICE has also worked cooperatively with the SSA for a number of years through the Systematic Alien Verification for Entitlements (SAVE) Program. The SAVE program enables Federal, state, and local government agencies to obtain immigration status information to determine an applicant or recipient's eligibility for many public benefits. The SAVE Program also administers employment verification pilot programs that enable employers quickly and easily to verify the work authorization of newly hired employees.

Current SAVE participants include the SSA; National Aeronautics and Space Administration (NASA); the Department of Defense Manpower Data Center; Arizona County Health Care Cost Containment; the California and Wyoming Departments of Motor Vehicles; the New Jersey Department of Law and Public Safety, Division of

Gaming Enforcement; the Mohegan Tribal Gaming Commission; and the Texas Department of Health, Asbestos Licensing Program.

The Secret Service has worked closely with the American Association of Motor Vehicle Administrators (AAMVA) to develop minimum and uniform standards for U.S. driver's licenses. I understand, for example, Mr. Chairman, that there are still four states that do not require a photograph on their state's driver's license, which, obviously, makes that document easier to use in a fraudulent manner.

Secret Service representatives work closely with the private sector on a number of efforts, and, together with the private sector, formed the Document Security Alliance as an ad hoc working group of law enforcement and industry focused on developing standards for the improving the security and traceability of plastic identification cards.

Conclusion

In sum, Mr. Chairman, DHS and BTS recognizes the enormity of the problems that we face, and we are working actively to improve our ability to detect fraudulent identification documents and to keep criminals and potential terrorists from obtaining these documents in the first place.

American Association of Motor Vehicle Administrators

Testimony of

Linda R. Lewis
President & CEO

American Association of
Motor Vehicle Administrators

Driver's License Security Issues

Submitted to the
Senate Finance Committee

Washington, DC

September 9, 2003

4301 Wilson Blvd, Suite 400 • Arlington, VA 22203 • Tel 703.522.4200 • Fax 703.522.1553
www.aamva.org

Good Morning, Chairman and distinguished Members of the Senate Finance Committee. My name is Linda Lewis and I am the president & CEO of the American Association of Motor Vehicle Administrators or AAMVA. Thank you for the opportunity to testify on behalf of AAMVA to discuss the vulnerabilities in the driver's license application process and the document itself, its impact on highway safety, identity fraud and national security and a comprehensive approach needed to fix the driver's licensing system.

AAMVA is a state-based, non-profit association representing motor vehicle agency administrators and senior law enforcement officials in the United States and Canada. Our members are the recognized experts who administer the laws governing motor vehicle operation, driver credentialing, and highway safety enforcement. AAMVA plays an integral role in the development, deployment and monitoring of both the commercial driver's license (CDL) and motor carrier safety programs. The Association's members are responsible for administering these programs at the state and provincial levels.

We believe this hearing will generate critical public discourse about the urgent public policy issue of building more integrity into the driver licensing process.

BACKGROUND

After reading the GAO report, neither I, nor any of my members, are surprised by the findings of the investigation. In fact, we believe this investigation is long overdue. This report, conducted under Congressional oversight, only adds to the mounting evidence that ***we need to fix*** our driver licensing process. As technical, hands-on authorities in this field, ***we can tell you*** that the report has, unfortunately, revealed only fragments of the problems that exist in driver licensing.

Why is this happening? Our current licensing structure and the credential that we issue were designed for another time and today's system is, at best, antiquated. The U.S. has more than 240 different, valid forms of passenger car driver's licenses and ID cards in circulation. Each state and D.C. has different practices for issuing licenses and reporting convictions. Individuals looking to undermine the system, whether a problem drinker, underage drinker, identity thief or terrorist shop around for licenses in those states with the weakest practices. Unfortunately, over-the-counter computer software and hardware is making it easier for individuals to produce counterfeit licenses and fraudulent breeder documents.

In addition, the lack of standard security features on a license allows individuals to exploit the system. This makes it difficult for law enforcement to verify the validity of a license from another state — not to mention the identity of the person holding it. This situation is worsened by the availability of counterfeit licenses and fraudulent breeder documents over the Internet and on the underground market.

AAMVA commends the Senate Finance Committee, for its focus on defining and showing the vulnerabilities with the driver's license and identification card. For over 70 years, the AAMVA membership has worked toward uniformity in driver licenses

practices. Our members have accepted that the driver's license—a credential, intended to provide the privilege to drive—has become America's most widely accepted form of ID within the past few decades.

Many of our members have taken steps to improve the driver's license issuance process within their own state borders. However, until we all share uniform practices, the process will remain fragmented and vulnerable ... as a result, we increase the opportunities for identity theft and put at risk our nation's national security and highway safety.

Shortly after September 11th, AAMVA members came together to develop a comprehensive solution to enhancing the licensing process. Note that I say comprehensive ... fixing one aspect of the problem ***will not*** make a difference.

This comprehensive approach addresses:

- tightened application requirements for obtaining a driver's license,
- real-time verification of an applicant's driver history and breeder documents,[1]
- improved processes and procedures for issuance, including internal audit controls and training for employees, and
- increased penalties for those that commit credential fraud.

Vulnerabilities & Comprehensive Approach

The events of September 11th, caused a radical shift in the perception of risk and the use of a driver license or ID card. In October 2001, the AAMVA Executive Committee developed and passed a resolution establishing the Special Task Force on Identification Security. The Task Force concluded that there were a number of common issues needing to be addressed: administrative processing, verification/information exchange, the need for a unique identifier, the format of the driver's license/ID card, fraud prevention and detection, residency, and enforcement and control of standards. Based on the recommendations of the Task Force, AAMVA brought together knowledge, experience and expertise from across jurisdictional boundaries, federal agencies and stakeholder organizations to establish uniform identification practices and procedures to aid in the prevention of fraudulently issued driver licenses and identification cards.

The objective, with participation and recommendations from states and provinces, was to provide a guide to jurisdictions that would help standardize the process of identifying applicants in the 21st century. AAMVA divided the issues surrounding identification security into 14 subtopics, each subtopic being addressed by a task group.

AAMVA has identified and targeted the areas to fix what we believe are the problems with the current system. Let's look at the vulnerabilities in driver licensing. And more importantly, the steps needed to tighten the system.

---

[1] Breeder documents are defined as those documents used to confirm identity such as birth certificates, Social Security cards or immigration documents.

First, individuals can apply for and obtain a license in more than one state, which the GAO investigators illustrated by using the same fictitious name and fraudulent documents in seven of the eight states. At this time, DMVs do not have an electronic method to verify whether a person has been issued a license in another state. We need to establish an information system that will ensure each driver has only one driver's license and one driver history record.

Currently, motor vehicle agencies use the National Driver Register/Problem Driver Pointer System (NDR/PDPS) maintained by National Highway Traffic Safety Administration (NHTSA). PDPS helps prevent the issuance of a driver's license to drivers whose licenses have been withdrawn or denied. States are supposed to query PDPS before issuing a license to an applicant to determine whether or not a given driver's license applicant has revocations, suspensions, denials or cancellations anywhere in the country. As illustrated by the GAO investigators, PDPS does not help DMVs determine whether a license has been issued by another state especially if the individual is presenting fraudulent documents and a fictitious name.

In the mid-1990s, AAMVA began exploring the possibility of having a system similar to the Commercial Drivers License Information System (CDLIS) for all drivers within the United States in order to better monitor the problem driver population. States need more effective tools to manage the driving records *we already maintain*. Problem drivers, who obtain multiple licenses, spread their bad driving history across the states. As a result, they avoid detection, penalties and punishment. By 1999, Congress recognized the potential benefits of such an information system and directed NHTSA and FMCSA to study the IT issues and costs associated with developing and operating this system. The report concluded an all-driver pointer system is feasible.[2]

We have witnessed the success of such a system through the use of CDLIS, which kept more than 871,000 potential dangerous truck drivers from obtaining a commercial driver's license between 1992 and 1996.[3] CDLIS is designed as a pointer system for commercial drivers. CDLIS limits commercial drivers to **one and only one** commercial driver's license and it has worked well for this purpose. Before CDLIS, it was possible for a commercial driver to apply for and obtain a commercial driver's license in a new state without acknowledging having an existing license in another state. This had serious implications for highway safety, since hiding the existence of another license could also hide a dangerous driving record.

We need an all-pointer driver system that will direct one state where to find and accurately verify someone's driving histories in other states for all drivers, commercial

---

[2] National Highway Traffic Safety Administration in conjunction with Federal Motor Carrier and AAMVA, "*Report to Congress: Evaluation of Driver Licensing Information Program and Assessment of Technologies,*" 2001. (http://www.aamva.org/drivers/drv_AutomatedSystemsDRIVerS.asp#Tech Assessment)

[3] Federal Highway Administration, Office of Motor Carrier Research & Standards Driver Division, "*Commercial Driver License Effectiveness Study,*" page 11, September 1998.

and non-commercial. DMVs already exchange driver history on commercial vehicle drivers through CDLIS. An all-driver pointer system will help prevent identity theft and strengthen national security by limiting a driver to one license and one driving history.

Second, the use of false breeder documents to obtain an authenticate driver's license or identification card runs rampant within the application process. DMVs must adopt a uniform resource list for acceptable identification documents, which will narrow down the numerous documents, relied on for issuing a license or identification card. After much research, AAMVA has recently concluded and issued the Acceptable Verifiable ID Resource List and Administrative Procedures.[4] By utilizing the lists, its procedures and future fraudulent document recognition training, motor vehicle employees should be able to verify that the applicant in front of them is who they are claiming to be and that documents presented are reliable. The use of the resource lists also promotes uniformity, identification reciprocity between jurisdictions, and helps protect the customer's personal information.

In addition, DMVs must provide adequate fraudulent document training to their employees. We need to give them the tools to recognize and appropriately handle fraudulent documents. The use of fraudulent documents has caused enormous economic losses in both the U.S. and Canada. The use of fraudulent documents to obtain driver's licenses/identification cards has grown exponentially in recent years. AAMVA in conjunction with the Federal Motor Carrier Safety Administration (FMCSA), the National Highway Traffic Safety Administration (NHTSA), the U.S. Secret Service (USSS), the Royal Canadian Mounted Police (RCMP) and the Canadian Council of Motor Transport Administrators (CCMTA) has developed a comprehensive model training program for Fraudulent Document Recognition (FDR).

The three-level FDR program is designed to assist states and provinces with the formal training of motor vehicle and law enforcement personnel in the recognition/detection of fraudulent identification documents. Level I address basic training needs for frontline employees and law enforcement officials. Level II addresses advanced training needs for motor vehicle supervisors, document examiners, law enforcement officials and fraud investigators. Level III addresses training at a forensic level and is slated for future development, if deemed necessary. Level I and Level II training materials were showcased during the 2003 AAMVA regional meetings. Formal Level I and Level II train-the-trainer sessions, designed to train jurisdictional fraud trainers, will be held between October 2003 and February 2004. Based on available funding, future development may include training videos, educational brochures, self-study materials and computer-based and/or Web-based training. AAMVA will establish a maintenance program to update the materials on a regular basis. We invite members of the committee to attend any of the upcoming training sessions.

---

[4] American Association of Motor Vehicle Administrators, *Status Report to AAMVA Membership-- Attachment 1 Acceptable Verifiable Resource Lists and Procedures*, July 2003,(http://www.aamva.org/Documents/idsAttach1StatReportJuly03.pdf).

Furthermore, we must ensure motor vehicle agencies have the ability, preferably electronically, to verify the validity of source documents with issuing agencies, such as the Social Security Administration, Immigration and Naturalization Services, vital records agencies and other DMVs. Currently, 25 states are electronically verifying Social Security Numbers with the Social Security Administration. But that verification process needs improvement. Too frequently SSA's automated system indicates that a number does not match, when in reality, after manual investigation, it is a match. This situation is deterring other states from using the SSA system. Congress must direct the Social Security Administration to improve their system so that this unnecessary, labor-intensive process can be eliminated. Each check of the system should also reference SSA's death records to ensure that a state does not issue a driver's license or identification card to an individual presenting personal information of a deceased person.

AAMVA is working cooperatively with the state and the Federal Motor Carrier Safety Administration (FMCSA) to pilot test three on-line verification systems:

- Online Verification of Driver Licenses – this allows states and third parties, such as airports and banks, to electronically verify that a license presented to them was actually issued by the state shown on the face of the license. Once rolled out nationwide, this effort will greatly inhibit a criminal's ability to use counterfeit driver licenses.

- Interstate Digital Image Exchange – this allows states to exchange digital driver photos so that they can compare the picture to the individual standing in front of the clerk applying for a license. Once rolled-out nationwide, this will inhibit imposters from obtaining licenses and ID cards under another person's identity.

- Online Verification of Birth Certificates – this allows the states to electronically interact with the National Association for Public Health Statistics and Information Systems (NAPHSIS) to check state vital statistics records to determine the validity of a birth certificate being used to establish identity as part of the driver licensing program. Once rolled-out nationwide, this will inhibit the criminal's ability to use counterfeit birth certificates to obtain a driver license or ID card.

These are very worthy efforts and, on behalf of the states, AAMVA thanks Congress and FMCSA for providing the seed money to get them going. But they are not fully effective unless all of the data is available and all of the states are participating. The states need the help and support of Congress to get these programs rolled-out nationwide.

Third, the driver's license document is easily counterfeited. The current variety of documents and lack of uniform security features makes it easy for criminals to alter a real document or create a counterfeit. We must provide fraudulent document training to not only DMV employees but stakeholders to thwart acceptance of fake documents. The GAO investigators showed how easy it was to create and alter a driver's license and breeder documents using inexpensive commercial available software and hardware.

Also, motor vehicle agencies must establish better procedures for removing fraudulent documents when an employee realizes the documents are fraudulent. We cannot afford to give the fraudulent documents back to the perpetrator and law enforcement needs to be notified without endangering the DMV employee. However in some instances, DMV employees inform individuals that produce fraudulent documents to obtain a driver's license or ID card the correct procedure to apply for a document. There is a delicate balance between customer service, safety and security.

Additionally, motor vehicle agencies need to adopt minimum, uniform card design and security specifications for the driver license document. To secure jurisdiction-issued driver's license/ID card credentials, the association examined card functionality, visible data and card layout, machine-readable data elements, machine-readable technology (MRT), document security features, and other card design elements and considerations. AAMVA, working with a wide variety of stakeholders, has developed those minimum specifications and they are now available for use by the states.

Fourth, we are all human. For some, this comes with the vulnerability to criminal behavior, which can result in stolen DMV equipment and inventory and the acceptance of bribes. Daily, individuals are breaking into DMV's, stealing equipment and inventory to produce documents. AAMVA is developing model procedures for security and inventory controls. DMVs and all identity issuing agencies need an information system to post alerts when equipment or inventory is stolen. Currently, through AAMVA's Web site, the association posts alerts regarding official federal, international or state documents and equipment that is stolen.

We must provide online verification of the driver license and ID card. This will render stolen equipment and inventory useless. Any driver licenses or ID cards created on stolen equipment would be rejected in the verification process because the state's database would not contain information pertaining to those cards.

Unfortunately, individuals bribe DMV clerks to issue driver's license or ID cards. It is a lucrative business. We want to stop criminal behavior on both sides of the counter. However, we need to implement stronger internal controls and auditing procedures that detect this behavior and prevent it from spreading. And, we must implement stiffer penalties and enforcement for those who choose to break the law.

Fifth, we must protect an individual's personal privacy while trying to bring the driver's license system into the 21st century. DMVs adhere to some of the strongest privacy laws on the books – the Driver's Privacy Protection Act. DPPA prohibits DMVs from selling your driver record information for commercial purposes without your prior consent. We'd like to make them stronger. The AAMVA Board of Directors passed a resolution stating that the association does not support the practice of collecting people's personal information from a driver's license for the purposes of marketing or building customer databases— without the full knowledge and consent of the license holder. We advocate that people or organizations scan the driver's license only to verify and not to capture information. Furthermore, in May 2003, the AAMVA Board endorsed eight

privacy principles based on the Global Privacy Design Principles.[5] The principles address openness, individual participation, collection limitation, data quality, use, disclosure limitation, security, and accountability. Therefore, AAMVA is assessing the impact of DL/ID security improvement on personal privacy and will develop best practices and model guidelines for motor vehicle agencies to inform citizens of personal information protection.

CONCLUSION

These problems exist and are **interstate** in nature. The only way to ensure that the proper fixes have been applied is for all states to follow the same roadmap. Inconsistent remedies from state to state will leave open the loopholes that exist today. The solution:

- must be implemented as a package and not as a piecemeal fix.
- will reduce identity theft and enhance homeland security and highway safety.
- can be accomplished ***without*** sacrificing an individual's personal privacy.
- can only be achieved with a federal-state partnership. Without a federal-state partnership to implement the solutions, this comprehensive approach is little more than a best practice.

Firsthand, you have witnessed the vulnerabilities of the current process. Congress, we need your help. AAMVA has submitted three proposals to Congress for authorization and funding to help implement this comprehensive approach through the reauthorization of the Transportation Equity Act for the 21st Century (TEA-21). We have asked for funding to implement an all-driver pointer system, interstate digital image exchange and online verification of birth and death records.

Now I ask you to take the first step in supporting the changes that must take place to reduce identity theft, enhance our national security and to save lives on our highways.

Thank you. I've concluded my testimony and welcome any questions from the subcommittee.

---

[5] American Association of Motor Vehicle Administrators, *Status Report to AAMVA Membership – Attachment 4 Privacy Principles*, July 2003, (http://www.aamva.org/Documents/idsAttach4StatReportJuly03.pdf)

Statement of the Honorable James B. Lockhart, III
Deputy Commissioner of Social Security
Testimony before the Senate Finance Committee
Hearing on the Homeland Security Threat from Document Fraud
Identity Theft and Social Security Number Misuse
September 9, 2003

Mr. Chairman and Members of the Committee:

Thank you for asking me to be here today to discuss issues surrounding document fraud, identity theft, and misuse of the Social Security Number (SSN). I am pleased to have the opportunity to tell you about the efforts that SSA has made to strengthen the integrity of the SSN, and to describe the SSN verification processes we have in place. I also want to discuss what we are doing to help states to verify the names and SSNs of individuals who apply for driver's licenses. The SSN is the single most widely used identifier for Federal and State governments as well as the private sector. As the number of uses for SSNs increases, especially in the private sector, so the potential for misuse of the SSN increases.

The tragic events of September 11, 2001, have brought home to all of us the need to strengthen the safeguards to protect against the misuse of the SSN. Since Commissioner Barnhart and I have been at the Social Security Administration, we have made protecting the SSN and strengthening the integrity of the processes used to assign these numbers a major Agency priority. We have made a number of significant enhancements in the last two years and will continue to look for ways to improve on the safeguards now in place.

History of the Social Security Number and Card

First, I would like to describe the history and the original purpose of the SSN and the Social Security card. Following the enactment of the Social Security Act in 1935, the SSN was developed to keep track of the earnings of people who worked in jobs covered under the new Social Security program. The rules regarding the assignment of SSNs to workers were published in Treasury regulations in 1936.

The Social Security card reflects the number that has been assigned to each individual who applies for an SSN. The card, when shown to an employer, assists the employer in assuring that earnings are reported properly. Public information documents issued early in the administration of the program advised workers to share their SSNs only with their employers. Initially, the only purpose of the SSN was to assure that SSA kept accurate records of earnings under Social Security so that we could pay benefits based on those earnings.

Use of the SSN Expands Over Time

Although the purpose of the SSN was narrowly drawn from the outset of the program, use of the SSN as a convenient means of identifying people in large systems of records has increased over the years. In 1943, Executive Order 9397 required Federal agencies to use the SSN in any new record systems for the purpose of identifying individuals. This use proved to be an early reflection of what has become an enduring trend to expand the use of the SSN. The simplicity and efficiency of using a unique number that most people already possessed encouraged widespread use of the SSN by both government agencies and private enterprises, especially as they adapted their record-keeping and business systems to automated data processing.

In 1961, the Federal Civil Service Commission established a numerical identification system for all Federal employees using the SSN as the identification number. The next year, the Internal Revenue Service (IRS) decided to begin using the SSN as its taxpayer identification (TIN) for individuals. In 1967, the Defense Department adopted the SSN as the service number for military personnel. At the same time, use of the SSN for computer and other accounting systems spread throughout State and local governments, to banks, credit bureaus, hospitals, educational institutions and other parts of the private sector. During this time, there were no legislative restrictions on the use of the SSN.

Statutory Provision Relating to the Public Sector

The first explicit statutory authority to issue SSNs was not enacted until 1972, when Congress required that SSA assign SSNs to all noncitizens authorized to work in this country and take affirmative steps to assign SSNs to children and anyone receiving or applying for a Federally funded benefit. This provision was prompted by Congressional concerns about welfare fraud and about noncitizens working in the U.S. illegally. Subsequent Congresses have enacted legislation which requires an SSN in order to receive Supplemental Security Income (SSI), Temporary Assistance to Needy Families (TANF), Medicaid, and food stamps. Additional legislation authorized States to use the SSN in the administration of tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction.

The Privacy Act was enacted in 1974 partly in response to concern about the widespread use of the SSN. It provided that, except when required by Federal statute or regulation adopted prior to January 1975, no Federal, State, or government agency could withhold benefits from a person simply because the person refused to furnish his or her SSN.

In the 1980s, new legislation provided for additional uses of the SSN, including employment eligibility verification, military draft registration, driver's licenses, and for operators of stores that redeem food stamps. Legislation was also enacted that required taxpayers to provide the SSN for each dependent age 5 or older. The age requirement was lowered subsequently, and an SSN is now required for dependents regardless of age.

In the 1990s, SSN usage continued to expand with legislation that authorized its use for jury selection and for administration of Federal workers' compensation laws. A major expansion of SSN usage was provided in welfare reform legislation enacted in 1996. Under welfare reform, to improve child support enforcement, the SSN was authorized to be recorded in a broad array of records, including applications for professional licenses, driver's licenses, and marriage licenses, divorce decrees, support orders, and paternity

determinations. In addition, the SSN is integral to the operation of the State and National New Hire Directories that were established in welfare reform to enhance collection of child support payments.

Use of the SSN by the Private Sector

Currently, there are no restrictions in Federal law on the use of the SSN by the private sector. Businesses may ask for a customer's SSN for such things as renting a video, applying for credit cards, obtaining medical services, and applying for public utilities. Customers may refuse to provide the number, however, the business may, in turn, decline to furnish the product or service.

Continuing advances in computer technology and the ready availability of computerized data have encouraged the growth of information brokers who amass and sell large volumes of personal information, including SSNs collected by businesses. When possible, information brokers store and retrieve information about an individual by that individual's SSN because it is more likely than any other identifier to maintain unique records for each specific individual.

Contemporary Challenges Regarding the SSN

As you can see, Mr. Chairman, use of the SSN is widespread in our society. This usage is the product of numerous decisions made over the years. The cumulative effect is to make the SSN an important element in establishing and maintaining an individual's identity in various record systems, and the ability of individuals to function in our society and economy. As a result, the SSN is prized by criminals who are intent on stealing another person's identity, or creating a false identity.

Accomplished identity thieves use a variety of methods to gain access to personal data. We at the Social Security Administration want to do whatever we can to help prevent identity theft and assist in the apprehension and conviction of those who engage in this crime.

Agency Response to SSN Misuse and Identity Theft

Validating requests for SSNs and issuing Social Security cards is a major workload for SSA. For fiscal year 2002, we issued 18 million Social Security cards, of which 12.4 million were replacement cards. Of the approximately 5.6 million new SSNs issued, over 1 million were issued to noncitizens, the vast majority of whom were issued an SSN because their immigration status authorizes them to work. Both the events of September 11, 2001, and the rapid increase in the incidence of identity theft have emphasized the importance of strengthening the administrative processes employed by SSA in assigning SSNs. In the fall of 2001, SSA formed a high-level team which has met regularly ever since to recommend and follow progress toward policy and procedural enhancements to strengthen our ability to prevent criminals from using SSNs and cards to advance their activities. Some of these initiatives have delayed the receipt of SSNs for some citizens and noncitizens. However, we believe these measures are necessary to ensure the integrity of the SSN issuance process and to assure that only those who are entitled to an SSN receive one.

Shortly after September 11, we began a cycle of retraining for all of our employees regarding the rules for enumerating individuals, with a special focus on the rules relating to noncitizens. We started with refresher training for all involved staff, and have followed on with additional periodic special training and management oversight.

We have eliminated a significant vulnerability in our enumeration processes relating to requests for SSNs from individuals who are not citizens of the U.S. The vulnerability stemmed from the ability of counterfeiters to produce high-quality replicas of immigration documents issued by the Department of Homeland Security (DHS). While we have always emphasized and continue to emphasize with our employees the importance of scrutinizing all immigration documents to identify those that are obviously fraudulent, we concluded that improvements in desk top publishing software made such scrutiny unreliable as a defense against counterfeit documents.

Therefore, on July 1, 2002, we began verifying with DHS any documents issued by them before assigning an SSN. We are able to verify most of these electronically. But if a record of the immigration document has not been established on DHS's electronic system, we request written confirmation from DHS that the documents submitted are bona fide. No SSN is assigned until the authenticity of the immigration documents has been verified. While verification of all documents has delayed SSN issuance to some noncitizens, we believe that such verification is an important step in ensuring the integrity of the enumeration process.

We have been successful in establishing a process, administered jointly by SSA and the Department of State, to assign SSNs and issue SSN cards to selected noncitizens as part of the process that allows them to enter the country as permanent residents. Under this process, known as "Enumeration at Entry (EAE)," the data required to assign an SSN, including verification of the individual's immigration and work authorization status, are provided to SSA by the Department of State (DOS) and the DHS (formerly INS).

We have also revised our verification processes with respect to young children. The vast majority of children receive an SSN through our "Enumeration at Birth (EAB)" program where parents can request an SSN at the same time that the child's birth is registered with the state vital statistics organization. Where an SSN is not requested through EAB, the parents must contact at the local Social Security office. Since parents generally need an SSN for various reasons in the first year of a child's life, such as listing a child as a dependent on a tax return, it is unusual for an SSN application to be delayed past that first year. In addition to verifying birth certificates that are suspicious for any reason, in June 2002 we began verifying all birth certificates with the issuing states for children age 1 and over. In some cases these verifications can be done electronically, in others a paper process is used. Again these verifications can delay issuance of the SSN, causing inconvenience to the parents, but we believe this process is valuable in ensuring that SSNs are not issued inappropriately.

SSA is leading a new government project to facilitate the verification of vital statistics such as birth records. "E-Vital" should reduce the cost and time it takes to verify both birth and death information. While we continue to look for ways to improve our current processes, clearly implementation of these linkages would facilitate our ability to verify birth certificates. E-Vital would reduce resources needed to do these verifications by eliminating the very labor intensive paper process and reduce or eliminate the extra time parents must wait to get an SSN. At the e-Gov 2003 Conference and Exposition in June, SSA received the Pioneer Award in the area of e-Government for the e-Vital program.

To test the feasibility of bringing a tighter focus overall on issues related to the assignment of SSNs, we opened a Social Security Card Center in Brooklyn, New York in November 2002. The center represents a joint effort between SSA, SSA's Office of the Inspector General and the DHS Bureau of Citizenship and Immigrations Services (BCIS). Employees from SSA work with staff from these agencies to bring together in a single office the technical and investigative perspectives of each of the participating agencies. The results have been encouraging, and we are considering whether additional card centers would be successful in other parts of the Country.

We have taken a number of steps to protect the privacy of people's SSNs when they receive correspondence from us. For example, since late 2001, we no longer include the first five digits of the SSN on Social Security Statements or on Social Security cost-of-living notices. Envelopes completely conceal SSNs when they are included in correspondence where an SSN is necessary. Further, the Department of Treasury plans to implement procedures in 2004 that will end the necessity of including on paper checks the SSN of the individual to whom the check has been made payable.

In our efforts to enhance the integrity of our enumeration processes and further reduce opportunities for fraud through misuse and/or improper attainment of SSNs, we proposed changing our evidence requirements for assignment of SSNs and by defining "valid nonwork reasons." In March 2002, SSA stopped assigning SSNs to noncitizens for the sole purpose of applying for a driver's license. We

would issue an SSN to noncitizens only if they were authorized to work or where needed for a federally funded or state public assistance benefit. This closed a loophole on noncitizens applying for drivers' licenses just to get an SSN. At that time, we issued a letter to Governors in advance of the change. We also notified the American Association of Motor Vehicle Administrators (AAMVA) of the change.

A lawsuit was filed in the U.S. District Court for the District of Columbia on behalf of nonimmigrants residing in Illinois and Alabama who were denied SSNs for drivers' license purposes (Iyengar v. B. Barnhart) 233 F. Supp. 221-5 (D.D.C.-2002). On November 26, 2002, the U.S. District Court issued a decision holding that the March 2002 change to our program instructions was invalid and that SSA must use notice-and-comment procedures to effectuate this change. As a result of that case, in December 2002, we reinstated our prior policy pending publication of the proposed change in the Federal Register.

On March 26, 2003, we published a proposed rule to allow us to resume the restriction on nonwork SSNs by announcing that we would define a "valid nonwork purpose" as those instances when a Federal statute or regulation requires a noncitizen to have an SSN in order to receive a federally-funded benefit to which the noncitizen has established entitlement, or when a State or local law requires an noncitizen who is legally in the U.S. to have an SSN in order to receive general public assistance benefits to which the noncitizen has established entitlement. In so doing, we will no longer issue an SSN so that a noncitizen may qualify to apply for a driver's license.

We also announced in that proposed rule that we would require an in-person interview with all individuals age 12 or older who are applying for an original SSN, and we will no longer waive the requirement to provide evidence of identity in original applications for a child under age 7.

The public comment period for these proposed changes ended on May 27, and we expect to implement these changes upon publication of the final rules.

Verification of SSNs

On an ongoing basis, SSA currently provides over 770 million SSN verifications a year to many thousands of different users, and the number of requests and users continues to grow rapidly. It is important to remember that when SSA receives a request for verification of an SSN, all we can really verify is whether the information included in the request, name, date of birth, etc., matches the information in our records for that SSN. Even if that information does match, it is no guarantee that the person presenting that SSN to the requesting agency or employer is in fact the person to whom that SSN was originally issued.

We have created a pilot of a web-based on-line system for employers to verify the names and SSNs of newly hired employees. This system, the Social Security Number Verification Service, is also known as SSNVS. It supplements other SSN verification systems that have been available to employers for more than twenty years. Currently, 69 companies have enrolled to participate in the pilot, and employers have used SSNVS over 8,800 times to verify over 1.7 million SSNs.

One of the services offered by SSA to certain government agencies that use the SSN is to verify SSNs that have been provided to them by individuals who have applied for services from that agency. A partial list of the various users of these verification services include:

- The Department of Education to verify the SSN's of individuals applying for federal student aid.
- State human services agencies for TANF, Medicaid, unemployment insurance, worker's compensation and pension coordination
- HHS, Office of Child Support Enforcement (OCSE) to manage their database of SSNs and new hires

- Prisons to verify the SSNs of inmates whose benefits should be suspended because of their incarceration
- The Office of the Inspector General (OIG) to assist in criminal and fraud investigations and to help track fugitive felons
- Department of Justice and state and local law enforcement agencies to assist in certain criminal matters and fraud investigations and to help track fugitive felons
- The Department of Veteran's Affairs for applicants for VA benefits and medical services
- The Department of Homeland Security for immigration purposes
- The Department of State for immigration purposes
- The Department of Defense for employees and military inductees
- Internal SSA users for purposes of administering benefits programs
- Federal Emergency Management Administration (FEMA) for emergency relief benefit coordination
- SSA provides SSN verification service to meet the needs of state Departments of Motor Vehicles.

Verification of SSNs for Driver's Licenses

While many of these verifications are geared toward preventing abuse of welfare and other cash paying benefit programs, the verification service we provide to the departments of motor vehicles are especially important with respect to the prevention of crimes related to identity theft and fraud. Since 1997, SSA has worked jointly with the American Association of Motor Vehicle Administrators (AAMVA) to provide an SSN verification service that is tailored to the needs of state Departments of Motor Vehicles (DMVs).

The SSA Online Verification Service (SSOLV) enables DMVs to request verification of an SSN from SSA while processing an application for a driver's license. Under this service, DMV employees enter the data necessary for verification through software maintained and administered by AAMVA. The software directs the request to SSA, where the information that has been entered by the DMV is to be compared to information housed in SSA's records for the individual who has applied for a driver's license. Requests are

received by SSA and returned in 1 second or less for 93 percent of these transactions. If our records indicate that an individual applying for a driver's license is deceased, we inform the DMV that there is an issue on our records that must be resolved with SSA. In addition to the online service, state DMVs may submit large numbers of drivers license records to SSA directly for verification. We refer to these as "batch" requests.

Currently, 34 states (including the District of Columbia) have entered into agreements to use the online service. Of those states, 22 states are using the online verification process and four states have begun testing their software with SSA. Nine states have agreements, but have not yet begun testing. (An additional state is testing with SSA but has not yet entered into an agreement). AAMVA plans to begin a renewed campaign to educate the states about the improvements to the process. In FY 2003, we estimate that we will process over 6 million requests from DMVs. AAMVA estimates that with the increased participation and improved systems performance, the number of requests processed in FY 2004 will be approximately 20 million. We expect our current, already low, cost of 3.4 cents per transaction to drop with this increased volume.

Unlike SSOLV, the batch process does not provide information that a death indicator exists in our records. Currently only seven states are using the batch verification process. The primary reason that they use this slower system seems to be cost. The General Accounting Office has recommended that SSA should modify the batch method to include a match against nationwide death records. We agree, and we are working to develop a remedy.

However, increasing the use of the online SSOLV system by the states is the best way to improve the integrity of the licensing system. First and foremost, it provides verification information to the MVA while the driver's license applicant is still at their counter. Negative verification gives the DMV the data it needs to prevent issuance of the driver's license. It is also the most efficient and cost-effective method for the states because it eliminates the need to issue temporary licenses while awaiting the results of the batch verification requests, a process used by some DMVs. This is why SSA is committed to pursuing and expanding the online service. It is

a system that works well, works quickly and ensures that fewer people will be able to obtain driver's licenses with fraudulent documentation.

Conclusion

I would like to conclude by emphasizing that we at the Social Security Administration are committed to strengthening the integrity of the processes that we use to assign SSNs. We believe the recent improvements we have implemented have made it more difficult for individuals to obtain SSNs from us through fraudulent means.

The difficult challenge we face is to balance SSA's commitment to assigning numbers quickly and accurately to individuals who qualify for them and need them to work, with the equally important need to maintain the integrity of the enumeration system to prevent SSN fraud and misuse. The President's budget request for FY 2004 includes the funding we need to continue our efforts to meet this challenge.

We have worked in the past and will continue to do so in the future with other Agencies—at the Federal, State and local levels—to assist them in making their processes less vulnerable to those who are intent on committing identity crimes. Together we can take action to thwart those who would abuse the SSN and other agencies' records to perpetrate identity crimes that burden Americans and threaten the security of our nation.

U.S. Senate
Committee on Finance

Statement for the Record

The Homeland Security and Terrorism Threat from Document Fraud, Identity Theft and Social Security Number Misuse

Patrick P. O'Carroll
Assistant Inspector General for Investigations
Social Security Administration

September 9, 2003

Good afternoon, Chairman Grassley, Ranking Member Baucus. Let me first thank you for the invitation to be here today for this important hearing on the homeland security and terrorism threat from identity theft, document fraud, and Social Security number (SSN) misuse.

The SSN as a National Identifier

Let me begin with a simple declaration: The SSN has become a national identifier. Two years ago, many people challenged that statement. Today, we live in a changed world, and the SSN's role as a national identifier is a recognized fact. The issuance of SSNs and driver's licenses based on invalid documentation creates a homeland security risk, and any failure to protect the integrity of the SSN can have enormous consequences.

Identity theft is the fastest-growing form of white-collar crime in the United States. Many expect that incidents of identity theft will more than triple from .5 million in 2000, to 1.7 million in 2005. While identity theft existed prior to the advent of the Internet, there is no question that in recent years, criminals have taken advantage of all of the readily available confidential information on the Internet. Some studies indicate that 10 percent of identity theft currently originates through the Internet. It is projected that by 2005 that number will rise to 25 percent. The proliferation of Internet-based information brokers also represents another resource for identity thieves. Most of these are third-party service providers, whose services help financial institutions track down deadbeat borrowers or conduct credit checks, are legitimate.

In most cases, identity theft begins with the misuse of the SSN. No aspect of the Social Security Administration's (SSA) Office of the Inspector General's (OIG) mission of protecting Social Security programs from fraud, waste, and abuse is more important than our oversight of the SSN. The SSN is so heavily relied upon as an identifier that it is a valuable commodity for lawbreakers. It can be obtained in many ways:

- Presenting false documentation to SSA.
- Stealing another person's SSN.
- Purchasing an SSN on the black market.
- Using the SSN of a deceased individual.

- Creating a nine-digit number out of thin air.

Identity fraud is a growing public concern, national in scope, and dangerous to both our economic health and our homeland security. Counterfeit identity documents such as those displayed in this hearing room remain a key component of identity theft. Identity theft is an "enabling" crime, one that facilitates other forms of crime. Those crimes may range from passing bad checks and defrauding credit card companies to acts of terrorism. In one case, a man stole the identities of 17 victims, and used them for credit card fraud, to purchase vehicles, horses, and other valuable items. One of the victims was the only U.S. Marine fighter ace to serve in both World War II and Korea, and another was a Hollywood actor. The identity thief was sentenced to 7 years in federal prison and ordered to repay $200,000 to SSA and $33,000 to the victims, though the total loss was $379,000.

Misused SSNs, stolen or misappropriated birth certificates, and false or fraudulently-obtained driver's licenses are the keys to identity fraud in the United States. With any one of these three documents, you can generally obtain the other two. We investigate thousands of SSN fraud and identity theft cases every year, and we often find the criminals have not only stolen or forged SSN information, but stolen or forged driver's licenses as well. We maintain a strong working relationship with the American Association of Motor Vehicle Administrators (AAMVA), and we have supported the development, deployment, and monitoring of the commercial driver's license and motor carrier safety programs throughout the United States.

Our Role in Homeland Security

While financial crimes involving SSNs are more numerous than terrorism-related crimes involving misuse of the SSN, the potential threat to homeland security nevertheless justifies intense concern.

Those connected with terrorism will at some point try to obtain SSNs. They may buy them, they may create them, or they may try to obtain them from SSA directly through the use of falsified documents. They need those numbers, and we must ensure that those numbers do not come from government agencies.

Our active involvement in homeland security began on September 11, 2001, with our agents assisting in rescue efforts and site security at the World Trade Center. We immediately assigned supervisors and agents to the FBI

Command Centers in New York City and New Jersey to process information and investigate leads. The Inspector General ordered all Field Divisions to assist in Joint Terrorism Task Forces (JTTF) and Anti-Terrorism Task Forces (ATTF) around the country—we are now active participants in 63 Joint Terrorism Task Forces and 29 Anti-Terrorism Task Forces, as well as the Foreign Terrorist Tracking Task Force and the Pakistani Task Force. We have participated in ATTF-sponsored homeland security projects focused on the Nation's critical infrastructure sites. Since 9/11 we have been involved in 132 such projects nationwide, to include 63 airports and 24 nuclear facilities, resulting in over 1,200 arrests.

By law and by mission, our office has a narrow but important role in this overall effort. Much of the Federal government response to identity theft issues rightly belongs to the FTC. State and local law enforcement agencies, and the financial institutions also have critical roles to play.

Since our primary mission is to protect the integrity of SSA's programs and operations, in the majority of our identity theft investigations, we continue to focus investigative efforts on cases that will affect SSN integrity. We continuously seek innovative ways to prevent SSN misuse and create collaborative partnerships with other Federal, State, and local entities. To maximize our investigative resources, we have dedicated agents to work in task forces with other law enforcement agencies to investigate identity crimes. We are working closely with prosecutors to bundle SSN misuse cases that, when presented separately, may not have been accepted for prosecution. The additional benefit of law enforcement agencies pooling their investigative resources is our ability to investigate more program and SSN misuse cases.

SSA issued approximately 18 million original and replacement Social Security cards in fiscal year (FY) 2002. We have found that SSNs have been issued to individuals using fraudulent documents. For example, an August 2002 audit estimated that during FY 2000, SSA assigned at least 63,000 SSNs to non-citizens based on invalid immigration documents that SSA processes did not detect. While SSA has improved its procedures in this area, we have no way of determining how many SSNs have been improperly assigned to non-citizens.

SSA has made significant progress in strengthening the defenses of the SSN, implementing important suggestions our office has made, and working with us to find solutions.

In May 2002, we issued a Management Advisory Report entitled Social Security Number Integrity: An Important Link in Homeland Security. That report stated that it is critical that SSA independently verify the authenticity of documents presented by SSN applicants. We also noted that SSA had established a task force to address some of these concerns, including improved verification procedures. For example, in September 2002 SSA started independently verifying all non-citizen immigration documents prior to issuing an SSN. We are currently assessing the Agency's compliance with these new procedures.

Protecting the integrity of the SSN has become a major part of the work we do. The FY 2004 President's Budget will allow us to begin staffing our SSN Integrity Protection Team to combat SSN misuse and identity theft. The Team is an integrated model that combines the talents of auditors, investigators and attorneys in a comprehensive approach, allowing SSA and OIG to:

- Support Homeland Security.
- Identify patterns and trends of SSN misuse.
- Locate systemic weaknesses that contribute to SSN misuse such as in the enumeration and earnings related processes.
- Recommend legislative or other corrective actions to ensure the SSN's integrity.
- Pursue criminal and civil enforcement provisions for individuals misusing SSNs.

Our SSN Integrity Protection Team will enable us to better target audit and investigative work. The Team will participate with other Federal, State and local entities to collaborate on potential SSN misuse activities. It is critical that we receive full funding in the President's Budget for FY 2004 in order to accomplish this important initiative.

Legislation is critically needed to strengthen SSN integrity

Legislation to strengthen SSN integrity is critically needed in three distinct areas our audit and investigative work identifies. The first area is limiting the use and display of the SSNs in the public and private sectors. Second, the present arsenal of criminal, civil, and administrative penalties need to be

strengthened to deter and/or punish identity thieves. The third approach is requiring the cross-verification of SSNs, which I will discuss further in a moment, to combat the spread of false of identification and limit SSN misuse.

Congress enacted the Identity Theft and Assumption Deterrence Act in 1998, responding to the growing epidemic of identity thefts by imposing criminal sanctions for those who create a false identity or misappropriate someone else's. The Internet False Identification Prevention Act, adopted in 2000, closed a loophole left by the earlier legislation, enabling our office and other law enforcement organizations to pursue vendors who previously could sell counterfeit Social Security cards legally by maintaining the fiction that such cards were "novelties" rather than counterfeit documents. More legislative tools are needed, and we have worked with Congress to identify legislation necessary to protect the integrity of the SSN.

The House is now considering H.R. 2971, which would seriously restrict the use of SSNs in the private and public sector, and criminalize the sale of SSNs. We have asked for an administrative safety net in the form of Civil Monetary Penalty authority for those instances of SSN misuse that could not be criminally prosecuted. We have also sought more meaningful criminal penalties in the Social Security Act for those few SSA employees who betray the public trust and assist criminals in obtaining SSNs. We are following the progress of H.R. 2971, and we would be glad to work with Senate Committee on Finance on such legislation.

We would like to explore the cross-verification of SSNs through both governmental and private sector systems of records to identify and address inaccuracies in SSA's files, and in data bases at various levels of government and the financial sector. Cross-verification can combat and limit the spread of false of identification and SSN misuse. All law enforcement agencies should be provided the same SSN cross-verification capabilities currently granted to employers. It would use data already available to the Federal, State and local governments and the financial sector.

The rewards of cross-verification can be impressive, yet it would not require major expenditures of money or the creation of new offices or agencies. Congress could pass legislation requiring mandatory cross-verification of identification data between governmental, financial and commercial holders of records and the SSA on a recurring basis. Commercial and financial

entities could be charged a modest fee-for-service to offset SSA's costs for providing this service. The technology to accomplish these data matches and verifications exists now. Coupled with steps already underway by SSA to strengthen the integrity of its enumeration business process, cross-verification, once initiated, would be a critical step in combating the spread of identity fraud.

We continue to work with Joint Terrorism Task Forces and Anti-Terrorism Task Forces participating in homeland security projects. We remain in constant contact with this and other committees of both houses of Congress to provide expertise and assistance in the analysis of data and creation of legislation aimed at protecting the SSN and preventing it from being used improperly. We have attorneys working either as Federal prosecutors or with them to enforce the Social Security Act's felony provisions. We continue our audit work, reviewing SSA's enumeration process and making recommendations for much-needed improvements. We are preparing to institute our SSN Integrity Protection Team to intensify and focus our efforts to combat SSN misuse and identity theft.

And we stand ready to do more. We appreciate your interest in these issues, and look forward to working with you to enhance the safety and well-being of all Americans.

Statement for the Record

Senate Committee on Finance
"Homeland Security and Terrorism Threat From Document Fraud, Identity Theft and Social Security Number Misuse"
September 9, 2003, 10:00 AM
Dirksen Senate Office Building, Room 215

John S. Pistole
Federal Bureau of Investigation
Acting Assistant Director, Counterterrorism Division

Good morning Chairman Grassley and members of the Committee. On behalf of the Federal Bureau of Investigation (FBI), I would like to thank the Committee for affording us the opportunity to participate in this forum and comment on the use of identity theft, document fraud, and social security number misuse and the potential nexus to terrorism.

Unfortunately, last week's *Washington Times* article regarding three Virginia men who filed numerous fraudulent labor certificates on behalf of Korean immigrants, who then used the bogus documents to obtain green cards to remain illegally in the US, is not something totally unheard of by Americans today. One of the defendants in this case used a fake social security account number to obtain credit cards, bank accounts and a driver's license. The Federal Trade Commission, just last week, released the first large government-sponsored survey on identity theft and stated the problem was far worse than officials had believed. Last year, identity theft cost consumers more than $5 billion in expenses, while costing banks and other businesses $48 billion.

As this Committee is well aware, the FBI, along with other federal law enforcement agencies, investigates and prosecutes individuals who use the identities of others to carry out violations of federal criminal law. These violations include bank fraud, credit card fraud, wire fraud, mail fraud, money laundering, bankruptcy fraud, computer crimes, and fugitive cases.

These crimes carried out using a stolen identity makes the investigation of the offenses much more complicated. The use of a stolen identity enhances the chances of success in the commission of almost all financial crimes. The stolen identity provides a cloak of anonymity for the subject while the groundwork is laid to carry out the crime. This includes the rental of mail drops, post office boxes, apartments, office space, vehicles, and storage lockers as well as the activation of pagers, cellular telephones, and various utility services.

Identity theft 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 identity theft as a separate and distinct crime problem. Rather, it sees identity theft as a component of many types of crimes which we investigate.

Advances in computer hardware and software along with the growth of the Internet has significantly increased the role that identity theft 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. The same multimedia software used by professional graphic artists is now being used by criminals and terrorists alike. Today's software allows novices to easily manipulate images and fonts, allowing them to produce high-quality counterfeit documents. The tremendous growth of the Internet, the accessability it provides to such an immense audience coupled with the anonymity it allows result in otherwise traditional fraud schemes becoming magnified when the Internet is utilized as part of the scheme. This is particularly true with identity theft related crimes. Computer intrusions into the databases of credit card companies, financial institutions, on-line businesses, etc. to obtain credit card or other identification information for individuals have launched countless identity theft related crimes.

The impact is greater than just the loss of money or property. As the victims of identity theft well know, it is a particularly invasive crime that causes immeasurable damage to the

victim's good name and reputation in the community; damage that is not easily remedied. The threat is made graver by the fact that terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated. Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fueling many of these methods.

For example, an Al-Qa'ida terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell. They kept purchases below amounts where identification would be presented. They also used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, etc. Extensive use of false passports and travel documents were used to open bank accounts where money for the mujahadin movement was sent to and from countries such as Pakistan, Afghanistan, etc.

While the 9/11 hijackers did not utilize fraudulent identification, they did obtain US identification cards in their names. These are "legitimate" identification cards, but they are not issued by any state or federal agency. Some of the vendors the hijackers received these cards from were involved in fraudulent identification cases--they were subsequently charged and arrested. Some of the hijackers did apply for, and receive, legitimate state identification cards and Driver's Licenses.

The FBI has seen other examples of document and identification fraud in our investigations related to terrorism, to include: 1) the April 2003 arrest of William Joseph Krar in Tyler, Texas. Krar is the subject of a fraudulent identification matter, which was initiated in August 2002 based upon information developed following the delivery of a package of fake identification cards to the wrong address. The package, which contained numerous false

identifications, had been mailed from Krar in Tyler, Texas to an individual in New Jersey, an admitted member of the New Jersey Militia. The identities included a Defense Intelligence Agency identification, a United Nations Observer Badge and a Federal concealed weapons permit; 2) Top Ten Most Wanted fugitive Clayton Lee Waagner was found to have in his possession fraudulent US Marshal's badges and a significant amount of equipment for making fraudulent identification cards, in addition to bomb making materials and large amounts of currency; and 3) The investigation of the bombing of the Oklahoma City Murrah Federal Building was a collaborative effort between by the FBI and many other federal, state, and local law enforcement agencies. The evidence developed and presented in court led to the convictions of both Timothy McVeigh and Terry Nichols by two separate juries of their peers. McVeigh and Nichols, like others planning to commit a criminal act, utilized aliases. McVeigh was also known to utilize fraudulent identification.

Investigation and interviews of detainees have included the following instances of fraudulent documents and use of false identification related to terrorism matters: 1) A Pakistani detainee who served as a doctor and guard for the Taliban was detained at JFK for attempting to enter US on a forged passport; 2) An Iraqi detainee purchased a false Moroccan passport for approximately $150.00 in US currency, and used it to enter Turkey where he was arrested; 3) An Algerian detainee requested asylum in Canada after entering that country on a false passport; 4) A Yemeni detainee acquired a false Yemeni passport and was able to get a Pakistani visa; and 5) An Algerian detainee obtained a French passport in an alias name and used it to travel to London. The cost for this false passport was 3,000 French Francs.

The FBI has implemented a number of initiatives to address the various fraud schemes being utilized by terrorists to fund their terrorist activities. One involves targeting fraud schemes being committed by loosely organized groups to conduct criminal activity with a nexus to terrorist financing. The FBI has identified a number of such groups made up of members of varying ethnic backgrounds which are engaged in widespread fraud activity. Members of these groups may not themselves be terrorists, but proceeds from their criminal fraud schemes have

directly or indirectly been used to fund terrorist activity and/or terrorist groups. By way of example, the terrorist groups have siphoned off portions of proceeds being sent back to the country from which members of the particular group emigrated. We believe that targeting this type of activity and pursuing the links to terrorist financing will likely result in the identification and dismantlement of previously unknown terrorist cells. Prior to 9/11, this type of terrorist financing often avoided law enforcement scrutiny. No longer. The FBI will leave no stone unturned in our mission to cut off the financial lifeblood of terrorists.

Another initiative has been the development of a multi-phase project that seeks to identify potential terrorist related individuals through Social Security Number misusage analysis. The FBI, through its Terrorist Financing Operations Section, is taking SSNs identified through past or ongoing terrorism investigations and providing them to the Social Security Administration for authentification. Once the validity or non-validity of the number has been established, investigators look for misuse of the SSNs by checking immigration records, Department of Motor Vehicles records, and other military, government and fee-based data sources. Incidents of suspect SSN misusage are then separated according to type. Predicated investigative packages are then forwarded to the appropriate investigative and prosecutive entity for follow-up.

I again want to thank you for your invitation to speak here today, and on behalf of the FBI, look forward to working with you on this very important topic.