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.