Testimony of
Boris F. Melnikoff
On Behalf of the
American Bankers Association
Before the
Special Committee on Aging
United States Senate
On
Identity Theft
July 18, 2002

Mr. Chairman, members of the Committee, I am Boris Melnikoff, a member of the American Bankers Association's Fraud Prevention Oversight Council and Consultant to the Regional President with BB&T in Atlanta, Georgia. I am here on behalf of the American Bankers Association to address industry efforts to protect consumers from the problem of identity theft.

ABA brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Our membership, which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks, makes ABA the largest banking trade association in the country.

Identify theft is on the rise. Stopping ID theft before it occurs and resolving those unfortunate cases that do occur is of utmost importance to the banking industry. Banks have a long and proud history of securing their customers' information. As technology and the Internet have made more information readily available – for better or worse – we have redoubled out efforts to help educate consumers about how to prevent and resolve cases of identity theft. Banks and our customers are partners in protecting information.

The Committee has asked us to outline current efforts on the part of banks to protect customers from identity theft. ABA is pleased to discuss these efforts as the education of consumers and the training of bank employees is crucial in detecting and preventing identity theft.

In my statement, I would like to make three key points:

- The banking industry has been actively involved in the ongoing effort to educate consumers on how best to protect themselves from being victimized by identify thieves. Consumer education begins with the recognition that each of us can limit our vulnerabilities to this crime.

- The American Bankers Association has developed many materials for our member banks – including videos, articles and statement stuffers – to assist in training bank personnel on identity theft prevention and to facilitate outreach programs in banks' communities.

- It is important for the private and public sectors to pursue technological innovations to improve individual identification techniques, beginning, for example, with improved standards for the issuance of drivers' licenses, in order to better combat identify theft at the time the thief seeks to profit from it.

Identity theft harms consumers, financial institutions and severely challenges law enforcement. The efforts mentioned below are only successful if these three groups work in tandem.

What is Identity Theft and What Can We Do to Stop this Crime?

In general terms, identity theft occurs when someone uses another's personal identifying information (name, address, social security number or other related information) to commit any of a wide array of fraud. This ranges from using another's name to obtain a cell phone or apartment lease, to using the information to open credit card accounts, obtain a mortgage, and even commit more heinous crimes such as terrorism.

In specific terms, according to the federal law covering this activity (18 USC § 1028), it is a crime for anyone to:

> Knowingly [transfer] or [use], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

Measuring the scope of identity theft is not an easy task. There have been a number of statements issued by law enforcement, consumer groups and the media attempting to measure the scope of the identity theft problem. For example, Attorney General John Ashcroft has stated that an "estimated 500,000 to 700,000 Americans have their identity stolen" each year. Regardless of the precise number of cases, one thing is clear: identity theft is a major concern to consumers and financial institutions alike, and all of us can do more to address this potentially devastating crime.

In 1997, when changes to Section 1028 were first being debated, the American Bankers Association was very supportive of efforts, led by Senator Kyl, to add additional tools to help bring perpetrators of ID theft to justice. ABA released a strong statement of support on this measure to Senator Kyl, pointing out: "As an industry that works with law enforcement in constantly combating fraud and other criminal acts against financial institutions, we are grateful for your interest in adding prosecutorial tools to this effort."

Unfortunately, even after the changes proposed by Senator Kyl were made to the federal law on identity theft in 1998 – ***which made it easier for law enforcement to bring an action in these cases*** – there was no appreciable increase in prosecutions. We were encouraged, however, by the Justice Department announcement in May that a nationwide effort, led by U.S. Attorneys has resulted in 73 criminal prosecutions for identity theft. Nonetheless, it appears that a primary reason prosecutions have not increased is because losses on typical identity theft cases have fallen below the dollar threshold set by law enforcement that would trigger their active involvement. Our industry remains concerned about those high thresholds that must be reached before an identity theft case is considered for prosecution. Therefore, we believe more needs to be done, and we applaud the Justice Department's recent initiatives in this area.

Banking institutions already dedicate substantial resources towards assisting law enforcement in its efforts, and continue to do more everyday. For example, banks have a new, affirmative duty to

report ID theft under the "Suspicious Activity Report" (SAR) regulations. This requirement (of the Financial Crimes Enforcement Network's (FinCEN)) to specifically file SARs on identity theft provides a vital avenue for reporting this crime.[1] This will not only help facilitate prosecutions, but will also provide better data on the extent and nature of the crime. This, in turn, will help focus the training for bank staff and give the government a better feel for where banks are finding this fraud. With this information, banks now have another means to assist identity theft victims in getting their cases reviewed by law enforcement.

The Banking Industry Has Been Actively Involved in the Ongoing Effort to Educate Consumers

The members of the American Bankers Association have been leaders in the private sector's push to educate consumers about how they can protect themselves. Central to prevention is the recognition that each of us can limit our vulnerabilities to this crime. We realize that people need our expertise and guidance to avoid being victimized. As several government agencies, such as the Federal Trade Commission, the United States Secret Service and the Postal Service have done, the banking industry has offered a number of tips to consumers on protecting one's personal information.

For example, on the following page, I have included many common sense precautions we can all take. This listing was written by Lynne Sanders of JP Morgan Chase & Co. for the May/June issue of ***ABA Bank Compliance Magazine.***

---

1 As the Treasury bureau charged with handling these reports, FinCEN has indicated: Criminal activity related to identity theft or pretext calling has historically manifested itself as credit or debit card fraud, loan or mortgage fraud, or false statements to the institution, among other things. As a means of better identifying and tracking known or suspected criminal violations related to identity theft and pretext calling, a banking organization should, in addition to reporting the underlying fraud (such as credit card or loan fraud) on a SAR, also indicate within the narrative of the SAR that such a known or suspected violation is the result of identity theft or pretext calling. Specifically, when identity theft or pretext calling is believed to be the underlying cause of the known or suspected criminal activity, the reporting institution should, consistent with the existing SAR instructions, complete a SAR, " See Special SAR Form Completion Guidance Related to Identity Theft and Pretext Calling, SAR Activity Review June 2001, pg. 37.

Precautionary Measures to Stop ID Theft[2]

The following list provides tips on how you — and your bank customers — can stop an ID theft before it happens. Proactive measures provide the best protection for your assets and your good name.

1. Do not give out financial information such as checking account and credit card numbers — and especially your Social Security Number — on the phone unless you initiate the call and know the person or organization you're dealing with.
2. Do not pre-print your driver's license, telephone, or Social Security numbers on your checks.
3. Report lost or stolen checks immediately. Also, review new checks to make sure none has been stolen in transit.
4. Store cancelled checks — and new checks — in a safe place.
5. Guard your personal identification numbers (PINs) for your ATM and credit cards, and do not write on or keep your PINs with your cards. You should also guard your ATM and credit card receipts. Thieves can use them to access your accounts.
6. Be creative in selecting personal identification numbers for your ATM and credit cards, and passwords that enable you to access other accounts. Do not use birth dates, part of your Social Security Number or driver's license number, address, or children's or spouse's names. Remember: If someone has stolen your identity, he or she probably has some or all of this information.
7. If you receive financial solicitations that you're not interested in, tear them up before throwing them away, so thieves can't use them to assume your identity. Shred or make unreadable any other financial documents, such as bank statements or invoices, before disposing of them.
8. Do not put outgoing mail in or on your mailbox. Drop it into a secure, official Postal Service collection box. Thieves may use your mail to steal your identity.
9. If regular bills fail to reach you, call the company to find out why. Someone may have filed a false change-of-address notice to divert your information to his or her address.
10. If your bills include suspicious items, do not ignore them. Instead, investigate immediately to head off any possible fraud before it occurs.
11. Periodically contact the major credit reporting companies to review your file and make certain the information is correct.

For a small fee, you can obtain a copy of your credit report at any time. (Please note that in some states or municipalities, you may be legally entitled to these reports free of charge. Check with the credit bureau when ordering the report.) The three major credit bureaus and their phone numbers follow:

Equifax	(800) 685-1111
Experian	(800) 682-7654
TransUnion	(800) 916-8800

[2] See Lynne Sanders, "Stopping ID Theft in It's Tracks," ABA Bank Compliance, May/June 2001, pgs. 35-39.

ABA members have worked diligently to see to it that these types of "ID Theft Primers" are communicated frequently to both customers directly and to bank employees for outreach to the community. One of the best resources to combat identity theft is self-awareness of how you can protect yourself. We believe that taking many of these small steps, while not eliminating identity theft, will diminish the frequency of this crime.

The American Bankers Association Has Developed Many Materials for Our Member Banks

Mr. Chairman, and members of the committee, with my long history in corporate security, I am very pleased to report that the banking industry and our leading trade group, the American Bankers Association, have been tremendous examples of how to increase awareness of this invidious crime.

- In 2000, the American Bankers Association distributed to ***all*** of its members an "ID Theft Communications Kit." This kit, available on the ABA's website, was designed to help bank employees deliver the message of ID Theft prevention to consumers throughout the country. The kit contains public service announcements, sample statement stuffers and a sample newspaper column that a bank official could tailor to his or her community. We have provided a copy of this kit to the Committee.

- In the same year, ABA distributed a Video News Release (VNR) to promote public awareness of identity theft that reached an estimated 28.6 million viewers. To reach radio listeners with the same message, ABA staff and bank officials presented prevention tips to an estimated 10.8 million listeners. For the print media, ABA distributed a column that generated 1,008 newspaper articles with a readership estimated to be nearly 41 million.

- On a continual basis, ABA offers separate statement stuffers for banks to use in mailings to consumers, with close to six million distributed across the country.

Moreover, the Association makes sure that its various banker-training programs include sessions on identity theft. For example, at the 2001 ABA Regulatory Compliance Conference, a three-hour session was held for compliance officers, attorneys and auditors on privacy, identity theft and information security. We duplicated that effort in June of this year at the 2002 event. Another training delivery mechanism, the phone briefing, has also been used to communicate the message on prevention. ABA has been fortunate to have representatives from the Secret Service and the nationally known identity theft trainer, Robert Douglas (President of American Privacy Consultants), to assist in these efforts. ABA has also sponsored Mr. Douglas to provide identity theft and pretext calling prevention-training seminars. I have attached an article that highlights the benefits of these seminars.

- The ABA has also created a web page devoted completely to fraud solutions, including a page with consumer tips on identity theft prevention/solutions, and has endorsed the FTC's "KnowFraud" education campaign. The website also provides important links to various agency websites that cover this type of fraud.

- Finally, the Association was able to take advantage of an excellent training video on pretext calling and identity theft produced by JP Morgan Chase & Co. ABA has repackaged that tape for broad distribution to our membership. To date, we have sent out over 1,200 of these tapes and continue to provide the product free of charge to ABA members. A copy of this tape has also been supplied to the Committee.

While the ABA has done considerable work in this area, we realize that individual industry efforts must continue. Fortunately, many of our members are engaged in similar efforts around the country. I continue to witness superb examples of industry outreach, a few of which I want to share with the committee:

- ***Bank of America and the National Consumers League***

  Bank of America has recently announced a customer protection campaign, created in partnership with the National Consumers League to help educate consumers about identity theft. The project, called the "Invasion of the ID Snatchers," includes public service

announcements, a web site with tips for avoiding identity theft, and a variety of other materials consumers can use to protect their privacy on the Internet and elsewhere.

The new web site includes tips for consumers on preventing and recovering from identity theft, as well as a very useful overview of common scenarios explaining how thieves steal personal information and what they are able to do with it.

In addition, Bank of America has also issued press releases on some broad-based e-mail scams. Media coverage resulting from the press releases have added value as they reach beyond the individual institution's customers to the public at large. ABA also urges the government to continue to issue fraud warnings through press releases and other communications to notify trade groups.

- ***California Bankers Association and Elder Abuse Prevention***

  A member of ABA's Compliance Executive Committee is chairing the California Bankers Association's task force on financial elder abuse prevention. They are working with a consortium that is producing an educational videotape for banks, as well as model procedures and policies. Similar efforts are underway in other states and localities.

- ***Commerce Bank and Trust (Topeka, Kansas)***

  Bank officials from Commerce Bank and Trust have given presentations to senior groups, including the Topeka Chapter of the AARP, on the various ways people can protect their personal information. In addition, the bank explains the process for credit reputation restoration and how to minimize fraud losses. This is just one example of hundreds of similar events occurring throughout the country.

- ***JP Morgan Chase & Co.***

  Several other large institutions have made identity theft outreach a major priority. In the previously mentioned ABA Bank Compliance article, JP Morgan Chase & Co. emphasized its education of both employees and the public. In 2000, JP Morgan Chase launched a nationwide awareness campaign that included both proactive and reactive measures. Two events are particularly important to cite. Programs were held in Houston and New York that

focused on elderly and minority members of those communities and the need to increase awareness of identity theft. Other participants included the U.S. Postal Inspectors Officer, the FTC, and AARP.

- ***Comerica***

  Comerica, based in Detroit, hosted an "Identity Protection Week" and developed a "Victim's Recovery Kit" which includes sample letters to credit bureaus and financial institutions, as well as a log for recording actions taken to report the crime. This type of assistance especially helps those who are unsure of how to manage the information minefields that accompany this fraud.

Improvement Needed for Issuance of Identification

Mr. Chairman, while there remains some debate on what other options exist to improve the ability of banks and consumers to protect consumers against ID theft and punish those that commit this crime[3], ABA urges consideration of new government leadership directed toward improving identifications. Specifically, the Congress should direct its attention to the nascent move to improve the current system of how states issue drivers licenses. There is no better way to protect against fraud and terrorism then by improving the identification documents used to complete financial and other business transactions. The American Association of Motor Vehicle Administrators (AAMVA) has offered an excellent outline of how to proceed. AAMVA has urged Congress, and ABA concurs, that there needs to be "minimum compliance standards and requirements that each state must adopt when issuing a license." We urge Congress to schedule additional hearings on this important topic as soon as possible.

Thank you for the opportunity to update the committee on our industry's efforts in the important area of educating the public on the identity theft issue.

---

[3] The Attorney General and the Chairman of the Federal Trade Commission have endorsed another proposal (S. 2541) that enhances the Federal law covering identity theft. The measure, among other things, creates a new crime of aggravated identity theft. If this change can help prosecutors take cases the industry certainly supports that goal.

ABA Bankers News℠
July 9, 2002
The Biweekly Newspaper of the American Bankers Association Volume 10, Issue 14

Article Reprint

Identity Theft Prevention Workshops

By Patrick Dalton

Because of the nationwide increase in identity theft and bank fraud, ABA has contracted with highly respected security expert Rob Douglas, CEO of American Privacy Consultants Inc., Oak Creek, Colo., to provide identity theft prevention workshops for banks. Tom Scalavino, group vice president/compliance officer at Compass Bank in New Bedford, Mass., recently hired Douglas to conduct a workshop for employees at his institution. ABA Bankers News asked Scalavino to talk about the workshop and some of the things the employees learned.

Scalavino

I truly believe that anyone who invites Rob Douglas to their bank to enhance identity theft training and pretext calling training will benefit immensely. I strongly recommend him.

Q. How did you hear about Rob?

A. I had read various articles quoting Rob on pretext calling.

bsequently, I met him at the ABA Compliance Conference in Washington, D.C., last year. That's how it all started. Pretext calling was one of the issues we were very concerned about. We felt his booklet from ABA on pretext calling ("Privacy and Information Security — An Awareness Guide") was very good, and we made it the basis for our initial in-house training. We also addressed various privacy issues with him. He was very knowledgeable. We asked Rob for his assistance on conducting pretext calling tests within the bank. Based on his experience and background, we felt Rob would certainly be of great assistance to us in pretext calling training and identity theft prevention training.

Q. How did the workshop work?

A. We invited Rob to New Bedford to conduct two three-hour sessions — one on April 10 and another on April 11. We encouraged individuals from every functional area of the bank — loan officers, loan processors, assistant branch managers and branch managers etc. to attend. The training was primarily for employees and officers whom we felt were in the front line of receiving calls that might compromise customer information security, if one was not properly trained nor sufficiently vigilant. Between the two sessions, about 140 employees attended.

Q. What are some of the things that jumped out at the employees?

A. I think they were alarmed as to how easy it is for someone to initiate pretext calls and impersonate someone else. They learned how certain individuals access the Internet to make false IDs. The ease of buying and sharing information on the Internet was very scary and quite enlightening to all of our employees. Rob demonstrated how information brokers pretend to be somebody else, such as claiming they work for an insurance company. They attempt to obtain some information from one employee, and then they call back and get more information from someone else. That was very informative to our personnel.

Rob also discussed several information broker stings he has been involved in. He showed a videotape spotlighting an information broker bragging on how easy it was to get information. The employees heard that, and I think it placed them on guard quite a bit more.

See Identity Theft/P

Identity Theft Prevention

From page 1

Q. What impressed you personally?

A. I had heard Rob speak at the ABA Compliance Conference, but actually seeing how the information is so easily and readily available for anyone who wants to impersonate someone else really got my attention. These people have no conscience. They are just out for the money, and they sell the information.

Rob went over the case of Amy Boyer, the Nashua, N.H., girl who was killed by a stalker after he paid about $220 to an Internet information broker to obtain the address where she worked. Amy's story really stood out and had a tremendous impact on everyone.

Q. Does the identity theft training have any implications for the terrorism issue?

A. Yes. The ease with which these individuals can create various identities and impersonate people has a tremendous impact on terrorism. It emphasizes how careful we must be in complying with established account-opening procedures to ensure that we identify the party in front of us. We must be very alert during every transaction, and be sure to know your customer. It is not simply obtaining an ID and quickly writing some information down by rote. It's making sure the description on the ID matches the individual in front of you. That's another important reminder folks walked away with — to be much more attentive during account-openings.

Q. What kind of reviews did Rob's presentation get from the employees?

A. I have 40 or 50 evaluations, and they are all along the same lines: "Excellent meeting." "Great information on a very serious subject." "I thought the presentation was very informative, and Rob is a fantastic instructor." Numerous employees thought the information also helped them personally — specifically, to be somewhat more cautious and a bit more protective of themselves, and to be more aware of their own accounts, their own surroundings and how they discard their personal mail.

Q. Would you recommend Rob's workshop to other bankers?

A. I truly believe that anyone who invites Rob Douglas to their bank to enhance identity theft training and pretext calling training will benefit immensely. I strongly recommend him.

For more information on the identity theft prevention workshops, go to www.privacytoday.com or call Rob Douglas at 970-736-1060.◆