

STOP I.T.!



*Let us help...
we're all in this together.*

A presentation designed for civic clubs, senior citizen groups, social organizations and similar audiences to be used in conjunction with the Georgia Bankers Association public awareness campaign to help stop identity theft and reduce fraud losses.



Georgia Bankers Association
www.gabankers.com

The Georgia Bankers Association is a founding member of the Stop Identity Theft Network, a public/private partnership that brings together federal, state and local officials with representatives of financial institutions and other businesses in an effort to stop identity theft in Georgia.

Hello. My name is _____ and I want to speak with you today about one of the fastest growing crimes in the country: identity theft. You've probably heard the term, seen news reports about the crime, or perhaps even known someone who's been a victim. Our bank has joined with other banks across the state who are also members of the Georgia Bankers Association to help get the word out about identity theft. We believe that with more knowledge and with just a little effort, we can all minimize our risks of becoming a victim of identity thieves.

Each of us works hard to make a living to support ourselves or our families. We all know the importance of keeping our credit reports clean so we can enjoy the benefits of that hard work. With a good credit history, we get quick access to credit when we need it and at economical rates and favorable terms.

What happens, though, when you learn that someone has used your name to get a credit card and has run up thousands of dollars in charges that you are now going to have to convince the credit card company that you're not responsible for? What if a bank account was opened or crimes were committed using your name?

Can you prevent this from happening? Can you protect yourself from these white collar criminals? What is law enforcement doing about it?

My purpose today is not to scare you or paint a worst case scenario for you. My purpose is to share some simple information with you and tell you about some real life examples just so you will understand how easy it is to fall prey to identity thieves. Hopefully, when you leave, you will be armed with some useful information you can use. You have a stake in protecting your good name and we have a stake in reducing the cost of fraudulent activity. I hope you will let us help because we're all in this together.

Identity thieves steal personal information, such as a credit card account number, Social Security number or driver's license number. Then they open up accounts in a consumer's name and run up charges on the account. Or, they use the personal information to charge goods and services to a consumer's existing accounts. In other cases, they may work, or even be arrested, while using the victim's name.

There are actually two types of identity theft (more correctly called identity fraud) and these are Financial Fraud and criminal activity.

Financial Fraud includes bank fraud, credit card fraud, computer and telecommunications fraud, social program fraud, tax refund fraud, mail fraud and several more. In fact, a total of 25 types of financial identity fraud are investigated by the United States Secret Service. Of the thousands of financial crime arrests made each year, more than 90% involve identity theft.

The other types of identity theft, however, usually involve a financial element as well – typically to fund some sort of criminal enterprise. These types of identity fraud involve taking on some else's identity in order to commit a crime, enter a country, get special permits, hide one's own identity, or commit acts of terrorism. These activities can include criminal and cyber crimes, organized crime, drug trafficking, alien smuggling and money laundering.

The harm to a consumer's credit and daily life can be devastating. Victims of identity theft often have trouble cashing checks, getting new credit cards or loans because of the damage to their credit ratings. According to the ID Theft Data Clearinghouse, the most common types of identity theft are:

- using or opening a credit card account fraudulently

- opening telecommunications or utility accounts fraudulently
- passing bad checks or opening a new bank account
- getting loans in another person's name
- working in another person's name.

The Federal Trade Commission reports that 9.9 million consumers were victims of identity theft in 2002 alone. The number of actual cases filed with the FTC is doubling every year, so the problem is real and growing.

Let me give you just three examples of actual people who were victims of identity thieves and how law enforcement determined their identities were stolen. I'll only use first names to protect the victims.

The first story is about Susan, a stay-at-home mom with two elementary school-age children. She came home one day and found a recording on her answering machine from a man saying the check she had written to buy his two Rottweilers had bounced and he was coming to her home to either get his money or the dogs. Susan had not bought any dogs and assumed the man had just dialed the wrong number and left the recording by accident. However, that night, a man appeared at her door demanding she make good on the check. You can imagine how frightened she was. But she was even more stunned when she saw the check in the man's hand that was identical to her own checks. Yet she had not written the check and didn't have a pair of Rottweilers to hand over to the man. After the involvement of Susan's bank, law enforcement and untold hours later, it was determined that someone had gotten a legitimate check she had written, scanned it into a PC and produced what looked like a check that any unsuspecting person would take. In fact, several more checks showed up over the next few days made out to a wide variety of individuals and businesses. No one was ever prosecuted for the crime, the man never got paid for his dogs, the other people who

got the fake checks lost their goods or the value of their services and Susan spent countless hours clearing her name.

Another story is about a woman named Alexandra who is a 40-year-old office equipment salesperson. She went to her ATM to withdraw some money and found her entire bank account had been drained. She subsequently learned that a woman somewhat matching her description had obtained a duplicate copy of her driver's license from an inattentive employee at the local department of motor vehicles. With that driver's license, the crook rented a car, had an accident and weeks later the car was found abandoned. The thief ended up not only creating havoc with her credit report, but Alexandra ended up with an arrest warrant pending for her for stealing a rental car. Her banker was able to quickly get her account back in order, but it took many months for Alexandra to clear up all the other matters.

The last victim's story is one that most of can relate to. Jim filled his gas tank at a local station and drove away forgetting to take the receipt that automatically printed out. A crook loitering around the station looking for just such an occurrence, simply walked up to the pump, took the receipt and ended up with all the information he needed to become Jim. He was even bold enough to look Jim's name up on the Internet and found his home address which was near the gas station. The crook applied for a duplicate credit card saying he had lost the original and began routinely checking Jim's mailbox. Within a few days, the duplicate credit card had arrived and the crook was off on a charging spree. The perpetrator was eventually apprehended and is now behind bars as part of a huge ring of thieves.

Every one of these victims was just like you or me. We go about our daily lives while criminals go about theirs. Think about it. In the course of a busy day, we may write a check at the grocery store, charge tickets to a ball game, eat at a restaurant, fill out a

survey on our computer, call home on our cell phone, order new checks or apply for a credit card. Everyday transactions that we may never give a second thought to are an identity thief's bread and butter. Each of these transactions requires the sharing of some sort of personal information: our bank or credit card account numbers, our income, Social Security number, or name, address and phone numbers, to name a few. While we can't prevent identity theft, we can minimize our risk by managing our personal information wisely.

(Note: depending on the audience and the time available, you may want to stop here and have those participating take a quiz to determine how likely they are to become victims of identity thieves. The quiz is at the end of this document. If you use the quiz, introduce it by saying something like:

You've heard three real-life examples of identity thieves. Let's take just a few minutes and test how well we are each doing in protecting our personal information. Read each statement on the quiz, and if that statement applies to you, circle the number at the end of the statement. When you've completed all the questions, add up the numbers circled. To see how well you're doing, compare your total score to the table at the bottom of the quiz to see where you stand.

After the audience completes the quiz, get back to your script by saying:

I won't ask for a show of hands, but from listening to some of the conversation around the tables, it sounded like some of us need to take action today!)

Let's get specific. What can you and I do to guard against becoming a victim? Here are just a few tips.

Before revealing personal identifying information, find out how it will be used and if it will be shared with others. Our bank and other financial service providers send you a statement every year telling you how we use the personal information you've entrusted with us. Make sure you read and understand that and demand it of others.

Pay attention to your billing cycles. Follow up with creditors if bills do not arrive on time. Your mail could be being stolen like in

Jim's story. Other people learn that some of their bills are being diverted to another address entirely. The earlier you find out about this, the better.

Give your Social Security number only when absolutely necessary. Ask to use other types of identifiers when possible. Georgia gives us the option of not using our social security number on our driver's license; take advantage of that option and use another number. Also, don't put your social security number on your checks. Congress continues to debate what to do about our social security numbers; but so far, no one has been able to come up with any other single identifier that works.

Minimize the identification information and the number of cards you carry to what you actually need. If you haven't taken everything out of your wallet or purse and made a photocopy of it, do so immediately. We all carry a lot of information around with us, even if we carry only the bare essentials. Having a photocopy of your wallet contents can help if your identity or credit cards are lost or stolen. You will need to quickly notify the creditors by phone, and call the three major credit bureaus to ask that a "fraud alert" be placed in your file. You can even add a "victim's statement" to your file requesting that creditors contact you before opening new accounts in your name.

Order a copy of your credit report from the three credit reporting agencies every year. Make sure it's accurate and includes only those activities you've authorized. In Georgia, these reports are free, so be sure and take advantage of that service.

Keep items with personal information in a safe place and tear them up when you don't need them anymore. Make sure charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards, and credit offers you get in the

mail are disposed of appropriately. Shredding is the best way to destroy these documents. Sure it's messy; but it's worth the effort.

Do not give out personal information over the phone if you did not initiate the call in the first place. Banks don't call their customers asking them to verify their account numbers and PIN numbers, yet these calls happen all the time. If you get a call from someone saying they are from your bank or the local hospital or any other business that has access to your personal information, don't answer any questions about that personal information. Also, you can help us catch the crooks if you get one of these calls and report it to your bank and to local law enforcement.

There are many more steps we can all take to minimize our risk of becoming a victim of identity theft, but when you think about it, all the tips are just simple common sense.

I don't want to leave you with the impression that even by taking all these steps, little can be done to stop identity thieves. That's certainly not the case.

Georgia was one of the first states to pass a law making identity theft a felony thanks to the leadership of Attorney General Thurbert Baker. The banking industry worked closely with General Baker on his initiative because we saw too many cases of identity theft going unpunished. By making identity theft a felony, prosecutors have more ammunition to go after the criminals and we are seeing many more successful prosecutions. The first legislation that passed only addressed consumers as victims. However, the Attorney General realized that businesses could also be victims; and at his urging, the General Assembly changed the law to now include businesses. Following Georgia's lead, in 1998, Congress passed legislation making identity theft a federal crime.

The Georgia General Assembly has also adopted two new laws recently that will help. For years, banks have followed rules which required the proper disposal of confidential information which was no longer needed. Most of this outdated material is shredded. The legislature has now put that requirement on all other businesses which have personal identifying information about us. This should help thwart identity thieves who rummage around in trash cans and dumpsters looking for information to steal.

Another bill passed the General Assembly will help, too. This bill prevents a person's full account number from being printed on a credit card receipt. There's a two year phase in to minimize the cost impact on merchants; but when fully implemented, cases like Jim's I told you about earlier won't happen.

We've also seen some successful prosecutions of identity thieves. The Attorney General's office has been able to consolidate several individual cases of identity theft and found a sophisticated ring of thieves. In one high-profile case in 2002, the Attorney General announced a guilty plea of one individual that led to the prosecution of several others. These crooks were involved in stealing thousands of pieces of mail from residential and business mailboxes. The ring then used the personal identification data obtained from the stolen mail to create fake drivers' licenses. They used the fake licenses to open credit accounts, bank accounts and charge accounts in their victims' names. What started out as well over a hundred individual cases of identity theft were consolidated into one case and the crooks are now behind bars.

At the federal level, the bank regulatory agencies are formalizing procedures that all financial institutions will follow should the information we have about our customers is compromised in any way. So far, these cases are extremely rare because of our long-standing practices of safeguarding customer information. Our track record is a good one and protecting our customer's

confidential information remains a top priority. We fully support these new standardized guidelines so all depository financial institutions will handle these matters in the same way.

In summary, let me say again how important it is for each of us to remain vigilant in guarding our personal information. There are a number of steps we can each take to minimize our risk of becoming a victim of identity thieves. We are fortunate that our elected leaders have taken proactive steps to support law enforcement and the prosecutors. Georgia is quickly becoming known as a state where identity theft is not tolerated. But if you suspect you've become a victim, take charge and take action. The longer you avoid the problem, the worse it will become.

I have a brochure* I hope you will take with you which will give you much more information. The banking industry in Georgia wants to ensure we've done our part by supporting positive legislative initiatives, by cooperating with law enforcement, by assisting our customers who are victims and by educating our community about the problem. Let us help...we're all in this together.

Thank you.

*Stop I.T. three-fold brochures are available for purchase at a nominal cost from the Georgia Bankers Association by calling Susie McGehee at (404) 420-2010. Alternatively, you may copy locally the one-page flyer included with this presentation which gives tips to avoid becoming a victim and instructions for victims.

Identity Theft – Are You at Risk?

Take the quiz below to raise your awareness and to determine your likelihood of becoming an identity theft victim.

Read each statement below **Circle point value if statement applies**

- I receive several offers of pre-approved credit every week5
 - Add 5 more points if you do not shred them before putting them in the trash5
 - I carry my Social Security card in my wallet.....10
 - I do not have a Post Office box or a locked, secured mailbox.....5
 - I use an unlocked, open box at work or at my home to drop off my outgoing mail.....10
 - I carry my military (or student) ID in my wallet at all times10
 - I do not shred or tear banking and credit information when I throw it in the trash10
 - I provide my Social Security number when asked without asking how the information is safeguarded.....10
 - Add 5 points if you provide it orally without checking to see who might be listening5
 - I am required to use my Social Security number at work or school as an employee or student ID number.....5
 - I have my Social Security number printed on my employee badge or student ID that I wear at work or show in public.....10
 - I have my Social Security number or driver’s license number printed on my personal checks.....20
 - I am listed in a “Who’s Who” guide5
 - I have not ordered a copy of my credit reports for at least 2 years.....10
 - I don’t believe people would root around in my trash looking for financial information ...5
- Total Points _____

100+ points:	You are at high risk. Take protective measures immediately (e.g. purchase a paper shredder, become more security aware in document handling and question why people need your personal data.
50-100 points:	Your odds of being victimized are about average; higher if you have good credit.
0-50 points:	Congratulations. You’re doing a good job of managing your personal information. Keep up the good work and don’t let your guard down.

STOP I.T.!



Let us help...we're all in this together.

Avoid Becoming a Victim of Identity Theft	Help for Victims of Identity Theft
<p>Identity Theft is reportedly the fastest growing consumer crime in the country. There are many simple steps you can take to protect yourself from becoming a victim.</p> <ul style="list-style-type: none">• Regularly check your bank and billing statements; if you see something you don't understand, call and inquire• Be careful not to carry personal information in your wallet or purse like your social security card, bank and credit card numbers with passwords and PINs• If you did not initiate the call, do not give out personal information over the phone• Leave your social security and driver's license numbers off your checks• Make sure your driver's license number is not the same as your social security number• Call your creditor if you haven't received a bill you were expecting• Use the post office or postal boxes for outgoing mail• Shred or otherwise dispose of receipts and other paperwork that contains any personal identifying information• Regularly order a copy of your credit report to check for unusual items• Destroy pre-approved credit card applications if you aren't going to take advantage of them	<p>The Federal Trade Commission reports in 2002 9.9 million people were victims of identity theft. If you are a victim, take these steps:</p> <ol style="list-style-type: none">1. Contact each of the credit reporting agencies to request a fraud alert be placed in your credit file.<ul style="list-style-type: none">• Equifax, P.O. Box 740250, Atlanta, Ga. 30374-0250, (800) 525-6285 or www.equifax.com• Experian, P.O. Box 1017, Allen, Texas 75013, (888) 397-3742 or www.experian.com• TransUnion, P.O. Box 6790, Fullerton, Calif. 92634, (800) 680-7289 or www.transunion.com2. Contact your local police or sheriff's department and make a report. Be sure to record the report number.3. Notify your bank and other credit grantors.4. Contact government agencies:<ul style="list-style-type: none">• The Federal Trade Commission is the national clearinghouse for identity theft information: (877) 488-4338 www.consumer.gov/idtheft• Governor's Office of Consumer Affairs: (404) 651-8600 or (800) 869-1123 www.ganet.org/gaoca



Georgia Bankers Association

The Georgia Bankers Association is a founding member of the Stop Identity Theft Network, a public/ private partnership that brings together federal, state and local officials with representatives of businesses and financial institutions in an effort to stop identity theft in Georgia.