The Many Ugly Faces of Identity Theft

Presentation at the 2003 Banking Institute
of the
University of North Carolina School of Law's
Center for Banking and Finance

By Wayne A. Abernathy
Assistant Secretary of the Treasury for Financial Institutions

April 10, 2003

Charlotte, North Carolina

This is something of a trip home for me, to come to Charlotte today. Or at least it's a trip home to my kin. My father was born just outside of Charlotte, in Davidson, here in Mecklenburg County. And he was raised just up the road, near Salisbury, in the little town of China Grove—not the Doobie Brothers' China Grove. And, like many people from China Grove, he worked for a time in the cotton mills, as did my aunts and uncles.

Besides an opportunity to join with me in reflecting and perhaps reminiscing, this information could be valuable to you. With this information and other information like it, you might be able to participate in America's fastest growing financial crime, the crime of identity theft. Not that anyone here would consider it, but I suspect that most of you here are concerned about it.

In fact, according to a recent survey, 90% of homeowners in America are concerned that somewhere, someone might use their good name to engage in fraud, to steal from a furniture store, rob a bank account, engage in stock swindles, write bad checks, run up huge phone bills, escape gambling debts, shield illegal drug deals, create false résumés, impersonate doctors or other professionals, destroy reputations.

Identity theft has many ugly faces. I want to expose some of them to you today, in the hope that awareness can put us on our guard and perhaps strengthen our resolve to fight this crime.

I begin with the dead. The dead are not immune from identity theft. Necrolarceny is one of the more repulsive, but not uncommon, faces of the crime.

Charlotte Smith Mecklenburg—I've made up the name, but otherwise I am reading from an obituary notice, found in newspapers in every community—age 77, died on Sunday, April 6, 2003. Wife of John Mecklenburg of State Street, Davidson, and mother of Wendy Mecklenburg Salisbury, of China Grove, North Carolina, and Robert J. Mecklenburg of Washington, D.C. Also survived by eleven grandchildren. A graduate

of Roanoke Valley High School, before becoming a cum laude graduate of Duke University, and continuing her chosen profession in art restoration at Johns Hopkins University. Involved in local Republican party politics, as well as the YWCA and Girl Scouts. Served on the Board of Directors of the American Society for Art Restoration.

Here, for all the world to read, is a deep well of information that an identity thief can draw from to impersonate Mrs. Mecklenburg, and probably get away with it for a good while. We know here an approximate date of birth, where she lived, where she went to school, her profession, her charitable activities, and names of family members. Chances are that Mrs. Mecklenburg is not going to be reading her financial statements for a while, and it is doubtful that closing Mrs. Mecklenburg's financial accounts is high on the To Do List of the bereaved family. Yet there might be a tragic surprise awaiting when the will of Mrs. Mecklenburg reaches probate and the family discovers how active she was financially in the days and weeks after her death.

But this obituary also points to potential victims among the living. We now know the mother's maiden name for Wendy Mecklenburg Salisbury of China Grove, North Carolina, and for Robert J. Mecklenburg of Washington, D.C., that is assuming that the "Smith" in Charlotte Smith Mecklenburg was the deceased's name at baptism, a pretty good guess. Until recently, mother's maiden name was one of those unique but little-known identifiers, used by financial institutions to validate customer identity. For this and other reasons, it is less relied upon today.

As an aside, a senior official at the Treasury gave my staff a Rumpelstiltskin challenge: discover his mother's maiden name within 24 hours. They did it.

Is this necrolarceny form of identity theft far-fetched, implausible? In May of last year a New Jersey woman received a notice from a North Carolina police department that her husband had just committed a traffic violation. The woman's shock gave way to renewed hope. Could it be that her husband, believed killed eight months earlier in the World Trade Center collapse, could it be that he had actually survived and somehow turned up in North Carolina? Unfortunately, her hope was dashed when she discovered that she had been terrorized once again, this time by a domestic criminal who used her deceased husband's identity as a shield to break the law.

According to more than one estimate, as many as a million people will become victims of identity theft this year. Many will suffer from the unauthorized use of their own legitimate credit card. This is one of the milder versions of the crime. As long as the consumer is diligent and promptly reports lost or stolen cards or unauthorized charges, the direct loss to the card holder is zero. The law sets the maximum loss at $50, but credit card companies have found that there are great benefits in consumer confidence from eliminating all liability for the innocent victim. The loss still occurs, though, and it adds up to billions each year, ultimately born by all card users in higher prices and higher interest rates.

Do not look for patriotism among identity thieves. Just as they show no pity to the victims of terrorism in New York, the identity thieves are likely poised to take advantage of the war. As our soldiers, sailors, and airmen move to the front lines to engage the enemy, the identity thieves are ready to move in to take advantage of the serviceman's absence from home to engage in fraud. I would guess that the soldier in the Third Infantry Division in Baghdad is not giving much thought to his bank account, or worrying about his credit cards, certainly not looking at his financial statements. But the fraudster is paying attention, for he knows that the fraud could go undetected for a long time, unless friends and family are vigilant, on the watch here at home over the financial affairs of the service man and woman overseas.

In the survey I mentioned, 12% of homeowners reported being victimized by identity theft, and 22% knew of a family member, friend, or acquaintance who was a victim. Undoubtedly, many in this room this afternoon have been victimized or know someone who has. Tragically, there may be some here who are being victimized right now and won't know of it for several more weeks or months.

Perhaps someone is dumpster diving, going through your trash to get important bits of information about you or your accounts. Perhaps someone will call, impersonating a government employee, asking to "verify" some of your personal data in order to continue to send you your Social Security check or veterans benefits. Maybe you will be snared by a supposedly "free" service on the Internet, that only needs your name, address, date of birth, and so on, in order to provide you with access to the free service. Or is there a very attractive charity asking for a check or credit card donation to help fight a terrible disease? All imposters, all ugly faces of identity theft.

So let us turn to one of the more virulent faces of this crime. This is not where a crook uses your legitimate credit card to make unauthorized purchases. This is where the crook takes your good name and uses it to open new accounts that you know nothing of, with the statements going to places you have never been, so that weeks and months pass without your knowledge of the fraud. The crook may even keep up minimum payments for a time until he can max out on the credit limits. Then he disappears, the payments stop and the creditors come looking. But they don't find the crook. They don't look for the crook. They look for you. And you discover the fraud when you can't pay for your dinner because your charge won't clear. Your home equity loan is turned down because there already is a lien on your house. You lose your job, because, though your boss is very sorry and thought you were an exemplary employee, he can't have someone in such a sensitive job who has such a poor credit history.

And then you find perhaps the ugliest face of all the ugly faces associated with the crime of identity theft, the face of the victim. Where do you go? How do you begin to clear your name? How do you convince creditors all around the country that you never made those transactions, that there must be some mistake? Do you turn to your local police department? They might fill out a police report, but many don't. What can the local police do about it anyway? The crime took place in Miami, not in your home town. Will the Miami police take up the case? Maybe, but you live in North Carolina. Who will

handle a case for a victim living in Charlotte, for fraudulent transactions made in Miami, Denver, and San Francisco, with money borrowed over the Internet from a bank headquartered in Philadelphia? You go to the federal authorities, you go to the FBI. How many millions of dollars were involved, they ask? You say, not millions, thousands, a lot of money to you. But the FBI has a lot of cases to handle, many much bigger than yours. How much time can they devote to your case of lost thousands?

So you the victim start down the long painful road of proving your innocence. The General Accounting Office reports that it can take victims as many as 175 man hours to clear their name and their records. That would be the equivalent of more than one full month of 8-hour days, five-day work weeks of full-time work. Of course, that is spread out over time, over months and sometimes years, with thousands of dollars of expenses.

No wonder that in that survey of homeowners, 83% said that government should do something to prevent this crime. We need to do something about it, or very important benefits of living in America will be in jeopardy.

We live in a country that offers to consumers the widest variety of financial services anywhere on earth, at the lowest cost anywhere on earth, to the broadest range of the population anywhere on earth. That is a marvelous achievement that we must not surrender.

This achievement is made possible by information, broad information, instantaneous information. Today, you can walk into practically any bank anywhere in America and obtain that very day a financial product suited to the needs of you and your family. And that is not just because the banker can look at your credit history and learn who you are, confident that he is getting the full story, but also because that banker can draw upon the information of a million people like you, and can define your risk and price it.

Some would say, "stop that information flow, that information is what feeds the identity thieves." But what would we give up? Who would we cut off from access to the home loan, the business loan, the college loan? It is true that when everyone in town puts their savings in the bank they make it easier for thieves to rob the community, all the money in one place—the crooks don't have to rob each house, one by one, they just rob the bank. But do we give up banks because the community's money is there, or do we make the banks more secure? Do we surrender the benefits we all enjoy from information sharing because crooks might use our information to harm us? Or do we provide for better security of that information, so that its use for our benefit is preserved?

We can stop the flow of information, but stagnant pools of information are of no more benefit than stagnant pools of water, and they are no more free from pollution. Instead, we can use information to fight the crime. The banker stops the identity thief when the banker knows more about his customer than the thief does. The police can catch the crook if information can jump state lines faster than the crook can. The victim's records can be restored if information on his clean record can be sent quickly to all parts of the nation.

These are some of the faces of identity theft. Not a pretty picture. But we need to face up to them and to recognize the danger to our modern, information-based economy. And rather than back away from the crime, we need to take it head on. To do that we need to recognize that it is not information that makes the crime possible. It is lack of information. The identity thief wears a mask. When the merchant or the banker can look behind the mask, and he knows what he sees, then we will strike a major blow at the crime. It is neither too soon nor too late to begin.