

# Profitwise

The Federal Reserve  
Bank of Chicago

Published by the Consumer and Community Affairs Division

Volume 12 Issue 2/ Summer 2001

## IDENTITY THEFT:

One of the

*Fastest Growing*

## CRIMES IN THE U.S.

**ALSO IN THIS ISSUE:**  
Finding Security in a  
Gramm-Leach-Bliley World

# Profitwise

*Profitwise* welcomes story ideas, suggestions, and letters from all bankers, community organizations and other subscribers in the Seventh Federal Reserve District. It is mailed at no charge to state member banks, bank holding companies and nonprofit organizations throughout the Seventh Federal Reserve District. Other parties interested in neighborhood lending and community reinvestment may subscribe, free of charge, by writing to:

*Profitwise*  
Consumer & Community Affairs Division  
Federal Reserve Bank of Chicago  
P.O. Box 834  
Chicago, IL 60690-0834

The material in *Profitwise* should not necessarily be interpreted as the official policy or endorsement of the Board of Governors of the Federal Reserve System, or the Federal Reserve Bank of Chicago.

**Advisor**

Alicia Williams

**Editor**

Michael V. Berry

**Assistant Editor**

Jeremiah Boyle

**Design**

Graphic Services

## In this Issue

- 1 Identity Theft: One of the Fastest Growing Crimes in the U.S.
- 2 Finding Security in a Gramm-Leach-Bliley World
- 3 Arts in Action for Affordable Housing

# IDENTITY THEFT:

One of the  
*Fastest Growing*  
CRIMES IN THE U.S.

JOHN W. CONNERY

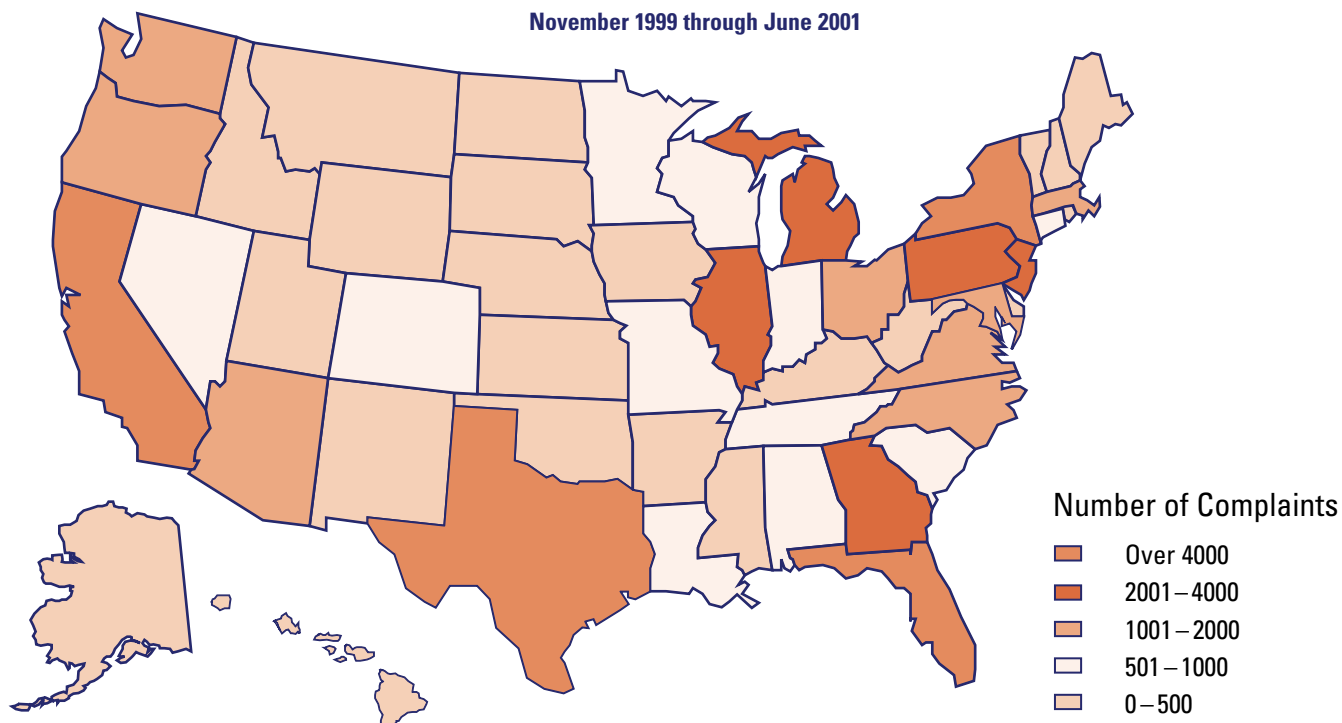
Consumer Regulations Director, Federal Reserve Bank of Chicago

**I**dentify theft” and “identity fraud” are terms used to refer to the fraudulent use of an individual’s personal identifying information. Typically, thieves will use stolen information, such as an individual’s name, address, Social Security number or account number in order to commit a financial crime such as check or credit card fraud. Identity thieves have also used stolen information to open investment accounts, obtain mortgage loans, rent apartments, establish utility service, cellular telephone service, and purchase expensive items such as jewelry, furniture and automobiles.

In some extreme cases, criminals have totally taken over another person’s identity. One notorious case involved a convicted felon who incurred more than \$100,000 of credit card debt, obtained a mortgage loan, and bought homes, motorcycles, and handguns in the victim’s name. The thief then filed for bankruptcy in the victim’s name.

## NUMBER OF IDENTITY THEFT COMPLAINTS BY STATE

November 1999 through June 2001



Source: Federal Trade Commission's Identity Theft Data Clearinghouse

Identity theft is one of the fastest growing white-collar crimes in the United States. The Federal Trade Commission (FTC) has tracked identity theft complaints since November 1, 1999 through its national identity theft clearinghouse. It received on average over 1,000 complaints per week during the months of July and August 2000. Approximately sixty percent of the calls were from victims reporting identity theft. The remaining forty percent of the calls were from consumers requesting information on ways to protect themselves from identity theft. More recent public statements by FTC officials indicate that the number of calls to the hotline have more than doubled since then, to over 2,000 calls per week. The Federal Bureau of Investigation estimated that last year more than 500,000 consumers were victims of identity theft and losses to consumers and merchants totaled \$1 billion.<sup>1</sup>

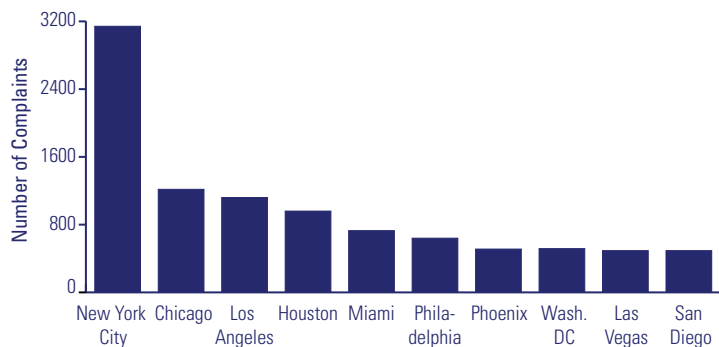
More than half of all identity theft crimes reported to the FTC last year involved credit card fraud. Thieves have run up debt in new credit card accounts that were opened using the victim's personal information. Criminals have also taken

over existing credit card accounts. Many of these crimes went undetected by the victim for months because the criminal contacted the credit card company to request a change of address on the account, thereby diverting billing statements from the true account holder. In many cases, the victims didn't realize that someone had stolen their identity until a creditor who was attempting to collect the unpaid credit card bill contacted them or when they were denied credit by another financial institution due to negative information on their credit report.

Check fraud also typically involves some form of identity theft. Many banks have reported that thieves have opened new checking accounts using personal information stolen from their customers. Another common scenario involves mail intercepts. Criminals have stolen victims' mail to obtain their bank checks. In other reported cases, identity thieves have impersonated the victim and requested a change of address for the account holder. Once new checks were printed with the change of address, they were sent to a mail drop rather than the true account holder's address. The thieves then

### CITIES WITH HIGHEST NUMBER OF COMPLAINTS

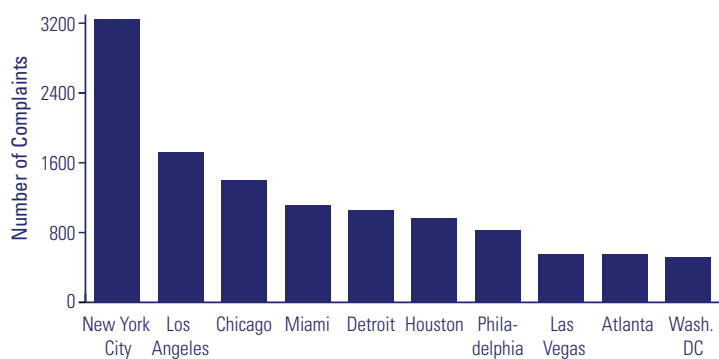
November 1999 through June 2001



Source: Federal Trade Commission's Identity Theft Data Clearinghouse

### CITIES WITH HIGHEST NUMBER OF SUSPECTS

November 1999 through June 2001



Source: Federal Trade Commission's Identity Theft Data Clearinghouse

wrote checks against the victims' accounts. The American Bankers Association (ABA) 1998 Check Fraud Survey found that \$3 out of every \$4 lost by a community bank to check fraud was due to some form of identity theft. In its 2000 Check Fraud Survey, the ABA found that attempted check fraud doubled in the past two years, exceeding \$2.2 billion. The report indicated that one-third of fraud cases and fraud losses were due to forgery.<sup>2</sup>

Although identity thieves can run up debts in the tens or even hundreds of thousands of dollars in a victim's name, several federal consumer laws and regulations as well as state laws limit consumers' liability for fraudulent transactions. In most cases, the victims of identity theft recoup all of their losses.

However, even though the victims may not be legally responsible for the debts, their credit history is often damaged. The victims typically must spend numerous hours over the course of months or even years contesting bills and correcting consumer report errors.

### WHAT'S DRIVING THE INCREASE IN IDENTITY THEFT?

Law enforcement officers have cited several reasons for the dramatic increase in identity theft: the increased availability of personal information in the market place, the ability of identity thieves to use this information in the market place, and the rapid and broad availability of credit.

Consumers routinely provide personal information to companies with which they conduct business. New computer technology has made it possible to transmit, store and analyze huge amounts of information. With the emergence of electronic commerce and the Internet in particular, personal information is collected and transmitted electronically around the world via the electronic web.

This information is a very valuable commodity. Many businesses manipulate it to target the consumers they believe will be likely purchasers of their products and services. Some companies swap or sell their customers' information to third parties. This trend has created an entirely new industry of information brokers that buy, sort, package and sell personal information to other businesses and individuals. These brokers not only buy and sell personal information from businesses, in some states they can purchase driver's license information, photos, birth and marriage data, as well as mortgage lien information.

Privacy advocates and law enforcement officers have raised concerns about how well these immense databases are being safeguarded. Anyone with a computer and a modem can access a variety of publicly available web sites with a significant amount of information about consumers. Many thieves have exploited this source of information. For instance, a Maryland couple who pled guilty in

1997 to running up over \$100,000 in debt using stolen identities admitted that they routinely used Internet databases to select their victims.<sup>3</sup>

A group of thieves used publicly available information from a government web site to impersonate a group of high-ranking military officers. The Congressional Record publishes the promotional list for high-ranking officers. The web site contained personal information about the officers including their Social Security numbers. According to the Secret Service, criminals used this information to fraudulently obtain credit, merchandise and other services. The criminals contacted a credit card company that agreed to issue credit over the Internet in less than a minute. Their applications were approved by the institution after it conducted a credit check that merely involved verifying that the applicant's name matched his or her Social Security number. Other information that was provided in the application, such as the applicant's date of birth, address and telephone number was false. Although the credit card company could have easily verified that the other information was inaccurate, in an effort to respond quickly to the consumer's application, the institution failed to conduct even a cursory check of the application information. As a result, the institution suffered substantial losses. The government now truncates the officers' Social Security numbers in order to protect their privacy.

Identity thieves are purchasing and obtaining under false pretenses data from information brokers and companies that collect personal data about their customers. According to law enforcement officials, data collection companies that do not carefully screen the individuals or businesses purchasing their data have become a convenient source of confidential customer information. And if they cannot buy the information, they may try to steal it. Law enforcement agencies have reported that cyber criminals continually demonstrate the ability to hack into merchants' nonpublic databases in order to steal customer information. In several instances, hackers that stole thousands of account numbers and other personal identifiers threatened to expose the crime unless the corporations paid them substantial sums.

The ability of the identity thief to purchase goods and services from innumerable E-merchants has dramatically altered the impact of identity theft. The explosion of financial services offered on-line provides a sense of anonymity to potential identity thieves whom would not risk committing a similar face-to-face transaction.

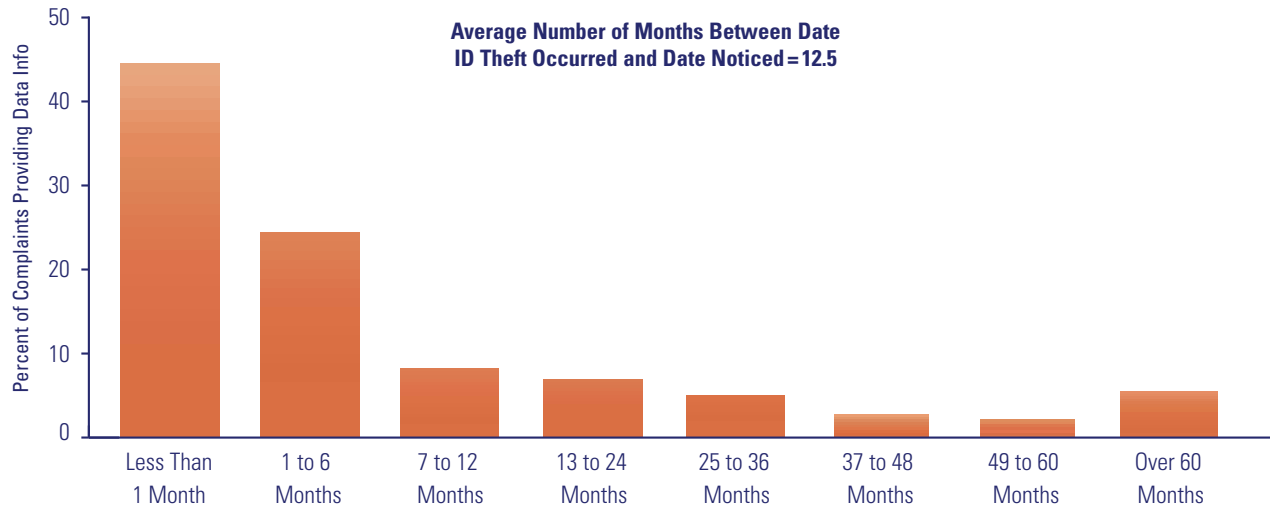
In order for financial institutions to be competitive, many are offering products and services that utilize new technologies such as ATMs, online banking and trading, E-commerce and smart cards. These products and services provide the anonymity criminals desire. In the past, fraud schemes required stolen or forged identification documents and a face-to-face meeting with an employee of a financial institution to open an account or conduct certain transactions. Criminals can now conduct a variety of financial crimes through a computer with stolen personal information.

### **COMBATING IDENTITY THEFT**

The dramatic increase in the number of identity theft cases prompted Congress to make identity theft a federal offense. The Identity Theft and Assumption Deterrence Act of 1998 criminalized fraud in connection with the unlawful theft and misuse of personal identifying information, regardless of whether it appears in or is used in documents. The new law accomplished several things. It identified the people whose credit had been compromised as victims in federal criminal cases and forced the courts to consider damages to these consumers and include them when fashioning restitution orders. Previously, only the merchant or creditor that assumed the financial loss was technically considered a victim of the crime. It provided stiffer penalties for perpetrators of identity theft. The law established the FTC as the central point of contact for victims to report all instances of identity theft. The new law also closed a loophole in the existing law, by making it illegal to steal another person's identification information with the intent to commit a violation. Previously, only the production or possession of false identity documents was prohibited. With advances in technology such as E-commerce and the Internet, criminals today do not need actual documents to assume a victim's identity.<sup>4</sup>

## NUMBER OF MONTHS BETWEEN DATE ID THEFT OCCURRED AND DATE NOTICED

November 1999 through June 2001



Source: Federal Trade Commission's Identity Theft Data Clearinghouse

The protection of financial information is a top priority for the financial services industry and their regulatory agencies. They have been working with local, state and federal law enforcement in an effort to reduce identity theft. New technological solutions have been developed to combat fraud involving companies that conduct electronic commerce. Many financial institutions have incorporated these tools. Many financial institutions have also taken steps to educate their customers about the risks of identity theft and precautions they should take to minimize their risk to this very invasive crime.

In addition, in January of this year the federal banking regulators—the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision—issued guidelines for safeguarding customer information.<sup>5</sup> The guidelines establish standards for banks relating to the administrative, technical and physical safeguards of customer information (see the article “Finding Security in a Gramm-Leach-Bliley World” by Gerald Jenkins). Banks are expected to take appropriate measures in accordance with the guidelines to protect customer information against identity theft. These guidelines became effective on July 1, 2001.

### HOW DO CRIMINALS ACQUIRE PERSONAL INFORMATION?

Thieves can obtain an individual's personal identifying information by methods as simple as stealing their purse or wallet, or as sophisticated as schemes involving the use of computerized databases or the bribing of employees with access to customer or personnel records.

The following are some examples of how personal information is obtained by criminals:

- Retrieving bank statements, deposit receipts, canceled checks, payroll stubs, account application information from dumpsters or trash bins (so-called “dumpster diving”);
- Stealing account statements and credit card solicitations from the consumer's mail box;
- Using telemarketing scams designed to trick consumers into revealing personal account information; and
- Obtaining the consumer's name, address and account numbers from checks given to retail businesses in payment for goods or services.

A new trend involves “group identity theft” where perpetrators target the workplace for employees’

## HOW IDENTITY THIEVES GET YOUR PERSONAL INFORMATION:

- *They steal wallets containing your identification and credit and bank cards.*
- *They steal your mail, including your bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information.*
- *They complete a “change of address form” to divert your mail to another location.*
- *They rummage through your trash, or the trash of businesses, for personal data in a practice known as “dumpster diving.”*
- *They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for—and a legal right to—the information.*
- *They get your business or personal records at work.*
- *They find personal information in your home.*
- *They use personal information you share on the Internet.*
- *They buy your personal information from “inside” sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services, or credit.*

personal information. In some cases, dozens of employees have found themselves victimized by a single offender or a ring of thieves. In one case of group identity theft, at the San Diego office of Ericsson, the wireless phone company, thieves used employee data stolen from the company’s personnel records to access eight employees’ online stock trading accounts and steal nearly \$700,000 in funds. A payroll employee at Ericsson’s headquarters was charged in the case. Other thieves then opened credit cards using at least 25 other employees’ personal information. The identity thieves ran up \$840,000 in credit card charges before the scheme was stopped.<sup>6</sup>

Identity theft is also becoming increasingly international; this fact is underscored by several episodes of intrusions into U.S. corporate databases by hackers operating in Eastern Europe and elsewhere around the world. The U.S. Secret Service has investigated a growing presence in this country of organized criminal groups, many with Russian or Nigerian origins, that have engaged in large-scale identity theft schemes targeting U.S. citizens.

On July 5, four Nigerian men were charged with leading one of the largest and most sophisticated identity theft frauds ever uncovered in Chicago. According to the U.S. Attorney, the group stole the identities of more than 2,300 people between May 2000 and May 2001. Using names, addresses, Social Security numbers and birth dates stolen from local companies, the ring allegedly opened bank accounts, applied for credit cards, and created counterfeit credit cards. The indictment further alleges that the ring went on shopping sprees buying more than \$2 million worth of computers and designer merchandise.<sup>7</sup> The merchandise was resold to third parties at half its original price.

According to authorities, the suspects obtained 200 pages containing personal information about 2,800 donors to a local blood bank.<sup>8</sup> They also obtained information about customers of other local businesses. The suspects apparently rummaged through corporations’ trash dumpsters in order to obtain some of the consumer information. However, the U.S. Secret Service is also investigating the

possibility that bribes were paid to employees of the companies for personal information about the credit card holders.

Armed with the information, the suspects created or applied for state-issued driver's licenses that were used to open bank accounts across the country. The indictment also alleges the ring created hundreds of counterfeit and unauthorized credit card account numbers and credit cards. Two of the suspects used computers to obtain and generate large numbers of actual, but unissued, credit card numbers. Some of the numbers were embossed on counterfeit credit cards and other numbers were used fraudulently to order and purchase goods and services over the Internet or by telephone.

The Secret Service also secretly tape-recorded one of the ringleaders, using various aliases, calling credit card companies to ask that replacement cards be sent to his new address and asking to increase credit limits on a number of credit cards. Another ringleader was recorded explaining how he used computers to access people's personal information and credit card numbers.

### ACCOUNT INFORMATION BROKERING AND PRETEXT CALLING

The tremendous demand for financial information regarding individuals and businesses has led to a dramatic increase in the number of companies specializing in the collection and dissemination of personal financial information. These so-called "information brokers" gather confidential information, including specific account numbers and balances, from various public and nonpublic sources. Bank account information collected by these brokers is often sold to attorneys, debt collection agencies or private investigators for use in lawsuits and other court proceedings.

Some information brokers use a technique known as "pretext calling" to obtain confidential customer information from financial institutions. Pretext callers contact financial institutions and use surreptitious or fraudulent means to try to coerce the employees into providing a customer's account information. For example, a broker armed with an

individual's Social Security number may pose as a bank customer who has misplaced an account number. The broker will repeatedly call the bank until he finds a bank employee willing to provide the information. The broker then sells the information to anyone who is willing to pay for it, including identity thieves. Identity thieves may also engage in pretext calling to obtain personal information for use in creating fraudulent accounts.

In a prepared statement presented to Congress on the issue of the use of deceptive practices to gain access to personal financial information, Al Schweitzer, of Al Schweitzer Investigations, described a hypothetical pretext call.

*"For example, if I wanted your bank account information Mr. Chairman (Rep. James A. Leach), I would first obtain your home telephone number either from the public records or if need be directly from the telephone company using another gag. I would then call the billing office of your local telephone company and claim to be you. At this point I know your name, address, telephone number and more often than not your Social Security number and date of birth. I would explain to the telephone company representative that although I know I paid my bill last month, I forgot to record it in my check register, I then ask "Could you please tell me how much it was and when it was due?" The service rep would then tell the amount paid and when it was due. Next I ask when my next bill is due and how much it is. The service rep would also freely tell me that. Now I change hats. I call you at home and I either get you or your wife on the telephone. This time, I'm the service rep at your local telephone company. Mr./Mrs. This is Mr. Sawyer with Bell Atlantic. I'm calling about your May bill that was overdue on June 10th in the amount of \$98.00. We haven't received payment and now your June bill in the amount of \$122.00 is also due. If this can't be paid immediately I'll have to disconnect your service. The majority of individuals will immediately become indignant, claiming that they have already paid those bills. Let me get my checkbook, here it is, I paid you on June 5th, \$98.00. You did? What check number was that? What bank was it drawn on? The account number please so we can locate it in our billing system. It was probably credited incorrectly to another account, I'm so sorry.*

## TIPS TO PREVENT IDENTITY THEFT

- *Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask if you have a choice about the use of your information; can you choose to keep it confidential?*
- *Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover his tracks.*
- *Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered.*
- *Put passwords on your credit card, bank, and telephone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number, or your telephone number or a series of consecutive numbers.*
- *Minimize the identification information and the number of cards you carry to what you'll actually need.*
- *Do not give out personal information on the telephone, through the mail or over the Internet unless you have initiated the contact or know whom you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers, and even government agencies to get you to reveal your Social Security number, mother's maiden name, financial account numbers, and other identifying information. Legitimate organizations with which you do business have the information they need and will not ask for it.*
- *Keep items with personal information in a safe place. To thwart an identity thief who may pick through your trash to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, bank checks and statements that you are discarding, expired charge cards and credit offers you get in the mail.*
- *Be cautious about where you leave personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.*
- *Find out who has access to your personal information at work and verify that the records are kept in a secure location.*
- *Give your Social Security number only when necessary. Ask to use other types of identifiers when possible.*
- *Don't carry your Social Security card; leave it in a secure place.*
- *Order a copy of your credit report from each of the three major credit reporting agencies every year. Make sure it is accurate and includes only those activities you've authorized. The law allows credit bureaus to charge you up to \$8.50 for a copy of your credit report.*

*There you have it Mr. Chairman, I now have your bank account information complete with your account number. Now I have two options. First, call the automated line of the bank where by entering your account number and Social Security number the automated attendant will provide dates and amounts of deposit and checks that have cleared as well as your balance. The second option would be to call a customer service representative and claim to be you, as I now have everything I need to impersonate you.”<sup>9</sup>*

Financial institutions that release information in response to a pretext phone call are not held liable under the Identity Theft and Assumption Deterrence Act. However, the financial institution and their customers who fall prey to pretext phone calling have the right to sue any person, including an information broker who obtains customer information in violation of the Act.

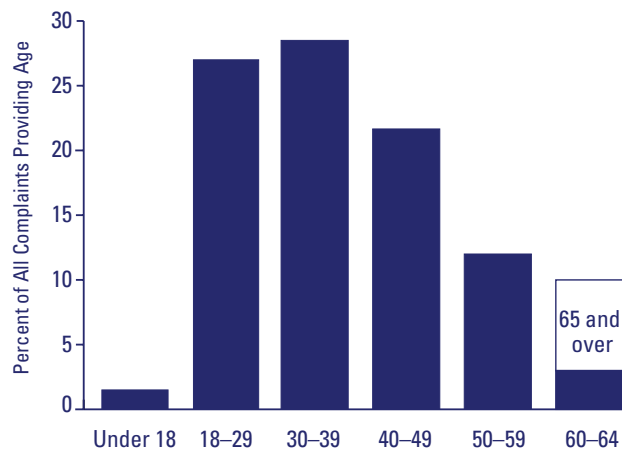
The Gramm-Leach-Bliley Act of 1999 (GLBA) made pretext calling a federal crime. The GLBA contained provisions that prohibit obtaining, or attempting to obtain, customer information from a financial institution by false pretenses.

In January, the FTC reported that they had conducted a “surf” of more than 1,000 Internet web sites and reviewed more than 500 advertisements in the print media for firms that offered to conduct financial searches. Based on this review, the FTC identified approximately 200 firms that offered to obtain and sell asset or bank account information about consumers. The FTC sent notices to these firms advising them that their practices must comply with the anti-pretexting provisions of the GLBA.

In April, the FTC announced that it had filed suit in three U.S. District Courts to halt the operations of information brokers who use false pretenses, fraudulent statements, or impersonation to illegally obtain consumers’ confidential financial information and then sell it. The FTC complaints alleged that these practices violate the FTC Act and the GLBA. The FTC also alleged that the sale of financial information obtained by pretext calling is likely to injure consumers by invading their financial privacy and exposing them to the risk of economic harm and financial fraud, because their information could be

## COMPLAINTS BY CONSUMER'S AGE

November 1999 through June 2001



Source: Federal Trade Commission's Identity Theft Data Clearinghouse

## HOW IDENTITY THIEVES USE YOUR PERSONAL INFORMATION:

- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.
- They open a new credit card account, using your name, date of birth and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- They establish telephone and wireless service in your name.
- They open a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they've occurred under your name, or to avoid eviction.
- They counterfeit checks or debit cards, draining your bank account.
- They buy cars by taking out auto loans in your name.

disclosed to individuals who might use it to deplete a bank account or liquidate a stock portfolio, or to steal an identity for other fraudulent purposes.<sup>10</sup>

### WHAT ARE THE MOST COMMON FORMS OF IDENTITY THEFT?

The most common forms of identity theft reported to the FTC during the first ten months the identity theft hotline was in operation were:

- **Credit Card Fraud**—Approximately 55 percent of consumers reported credit card fraud. Seventy-two percent of the complaints involved the establishment of a new credit card account in the victim's name and 24 percent involved the takeover of an existing account.
- **Communications Services**—Approximately 28 percent reported that the identity thief opened up telephone, cellular, or other utility service in the victim's name.
- **Checking or Savings Accounts**—Approximately 18 percent of the victims reported that a checking or savings account had been opened in their name. Forty-four percent of these reports involved the use of unauthorized checks, 28 percent involved the establishment of a new checking account in the victim's name and 19 percent involved an unauthorized electronic funds transfer.
- **Fraudulent Loans**—Approximately 11 percent reported that the identity thief obtained a loan, such as a car loan, in the victim's name.<sup>11</sup>

### VICTIMS OF IDENTITY THEFT

Many victims of identity theft have reported that they have spent a significant amount of time and expense resolving problems related to unauthorized accounts or transactions. In May 2000, the California Public Interest Research Group and the Privacy Rights Clearinghouse, a nonprofit advocacy group located in San Diego, released a joint survey of identity theft victims that had recently contacted their offices.

The survey identified the following patterns:

- Forty-five percent of the victims considered their cases to be solved. It took an average of 23 months to solve the cases.
- Seventy-six percent of the victims reported that identity thieves used their personal information to fraudulently open new accounts in the victim's name. The thieves on average opened six fraudulent accounts.
- The average total fraudulent charges made on the new and existing accounts of the victims surveyed was \$18,000.
- Victims spent an average of 175 hours and \$808 trying to resolve the problems caused by their identity theft.<sup>12</sup>

Many consumers have also reported problems with banks and other financial institutions that provided credit, goods, or services to the identity thief in the consumer's name. Victims complained that institutions often attempted to collect the bad debt from the victim, or reported the bad debt to a consumer reporting agency, even after the victim believed that he or she has demonstrated the fraud to the institution.

Victims of identity theft also expressed dissatisfaction with credit reporting agencies. Many victims reported to the FTC complaints of inadequate assistance when the consumer reported the fraud to the credit reporting agency. Many also complained that the agency did not reinvestigate or correct an inaccurate entry in the consumer's credit report.



# Consumer Rights

*The following are federal laws that provide rights and protections to victims of identity theft and its related financial crimes:*

## **IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT OF 1998**

In October 1998, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) to address the problem of identity theft. Specifically, the Act amended 18 U.S.C. § 1028 to make it a federal crime when anyone that knowingly transfers or uses, 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.

## **FAIR CREDIT BILLING ACT**

The Fair Credit Billing Act establishes procedures for resolving billing errors on “open end” credit accounts, such as credit cards, revolving charge accounts—such as department store accounts—and overdraft checking accounts. It does not cover installment contracts—loans or extensions of credit you repay on a fixed schedule. The Act also limits a consumer’s liability for fraudulent credit card charges to \$50.

## **FAIR CREDIT REPORTING ACT**

The federal Fair Credit Reporting Act (FCRA) establishes procedures for correcting mistakes on your credit record and requires that your record only be provided for legitimate business needs.

The Act gives consumers specific rights. You can dispute inaccurate information contained in a report prepared by a consumer reporting agency (CRA). If you tell a CRA that your file contains inaccurate information, the CRA must investigate the items (usually within 30 days) by presenting to its information source all relevant evidence you submit, unless your dispute is frivolous. The source must review your evidence and report its findings to the CRA. The source of the incorrect information also must

advise national CRAs, to which it has provided the data, of any error. The CRA must give you a written report of the investigation and a copy of your report if the investigation results in any change.

## **FAIR DEBT COLLECTION PRACTICES ACT**

The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that your creditor has forwarded for collection.

## **ELECTRONIC FUND TRANSFER ACT**

The Electronic Fund Transfer Act provides consumer protection for all transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer’s liability for unauthorized electronic fund transfers.

If you report an ATM or debit card missing before it is used without your permission, the Act says the card issuer cannot hold you responsible for any unauthorized withdrawals. If unauthorized use occurs before you report it, the amount you can be held responsible for depends upon how quickly you report the loss to the card issuer. If you report the loss within two business days after you realize your card is missing, you will not be responsible for more than \$50 for unauthorized use.

However, if you do not report the loss within two business days after you realize the card is missing, but you do report its loss within 60 days after your statement is mailed to you, you could lose as much as \$500 because of an unauthorized withdrawal. And, if you do not report an unauthorized transfer or withdrawal within 60 days after your statement is mailed to you, you risk unlimited loss. You could lose all the money in your account and the unused portion of your maximum line of credit established for overdrafts.

# Steps to Take if You Believe You Are a Victim of Identity Theft

## CONTACT YOUR FINANCIAL INSTITUTIONS IMMEDIATELY

Financial institutions could include banks, brokerage firms, credit card companies, as well as telephone companies and other utilities. Immediately contact these companies by telephone to report your suspicions. Customer service or fraud prevention telephone numbers can generally be found on your monthly statements. Always follow-up your calls with a letter. Close any accounts that have been tampered with and open new accounts with new personal identification numbers (PINs).

## CONTACT THE CREDIT BUREAUS AND CHECK VERIFICATION COMPANIES

Contact each of the three major credit bureaus and request a copy of your credit report. Review your reports to determine if any fraudulent accounts have been opened in your name or if any unauthorized changes have been made to your existing accounts. If any unauthorized activity is identified, request that a “fraud alert” be placed in your file, as well as a victim’s statement asking that creditors call you before opening any new accounts or changing your existing accounts. Also check the section of your report that list “inquiries.” Where inquiries appear from the company(s) that opened the fraudulent account(s), request that these inquiries be removed from your report. In a few months, order new copies of your credit reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.

*The three major credit bureaus are:*

Trans Union (800)680-7289  
Experian (888)397-3742  
Equifax (800)525-6285

If your checks were stolen, contact the major check verification companies. Request they notify retailers using their databases not to accept any of the stolen checks.

*Three of the check verification companies that accept reports of check fraud directly from consumers are:*

Telecheck (800)710-9898  
International Check Services (800)631-9656  
Equifax (800)437-5120

## FILE A POLICE REPORT

File a police report with your local police or the police in the community where the identity theft took place. Obtain a copy of the police report or the police report number. The police report may initiate an investigation into the loss and it will be helpful in explaining to creditors that you were a victim of identity theft.



## CONCLUSION

Identity theft is a serious and growing problem. Although there are steps one can take to minimize the risk of becoming a victim, there is no way to guarantee the security of personal information. The first step to reduce the overall risk is to take a more active role in protecting personal information.

Do not provide personal information to anyone over the telephone, through the mail or over the Internet unless you initiated the contact or you are sure that you are dealing with a representative of a legitimate business. Before you share any of your personal information, ask the company that you're dealing with for a copy of their privacy policy. If you're uncomfortable with their information sharing practices, don't establish a business relationship with them.

Banks, their regulatory agencies and law enforcement have taken steps to address and combat identity theft. Despite these measures, identity thefts involving customers of financial institutions continue to increase. Heightened awareness of this issue and the measures consumers and financial institutions can take to reduce the occurrence may be the most effective deterrent. Financial institutions are also encouraged to develop stronger fraud prevention practices and consumer assistance techniques.

Identity theft victims often need assistance in determining steps they should take to repair the damage to their credit record, reputation or other matters. Financial institutions should refer these individuals to the FTC, which can provide them with steps they can take to inform credit reporting agencies, credit issuers, law enforcement authorities and other agencies of the improper use of their identification information. The FTC will also provide the public with additional educational information recommending steps to be taken to prevent individuals from becoming victims of identity theft.

If a financial institution suspects an illicit attempt has been made to obtain a customer's identity information, it should immediately report the matter to the proper authorities. In such circumstances, institutions are encouraged to file a Suspicious Activity

Report, and contact their primary federal regulator, the FTC, and the appropriate state agencies charged with enforcing laws against identity theft. In addition, institutions should directly contact the appropriate law enforcement agencies if the situation appears to require immediate attention.

## ENDNOTES

<sup>1</sup>Greenberger, Robert S. and Glenn R. Simpson, "Identity Theft Dogs Credit Firms in the Supreme Court, Congress," *Wall Street Journal*, April 12, 2001.

<sup>2</sup>American Bankers Association, "1998 Check Fraud Survey" and "2000 Check Fraud Survey," [www.aba.com](http://www.aba.com).

<sup>3</sup>Prepared Statement of the Federal Trade Commission on "Identity Theft" before the Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary, 105th Cong. (1998) (statement of David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, FTC).

<sup>4</sup>Prepared Statement of U.S. Secret Service: Hearing on H.R. 4311, the "Identity Theft Prevention Act" before Comm. On Banking and Financial Services, House of Representatives, 106th Cong., 2d Sess., September 13, 2000 (statement of SAIC Bruce A. Townsend, U.S.S.S.).

<sup>5</sup>Federal Reserve, Interagency Guidelines for Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8616, [www.federalreserve.gov](http://www.federalreserve.gov), February 1, 2001.

<sup>6</sup>Ted Leventhal, "Identity Theft On Rise, Says FTC Official; Employees Targeted by Identity Thieves," *Privacy Times*, July 26, 2000.

<sup>7</sup>United States Department of Justice, U.S. Attorney-Northern District of Illinois, Press Release: "Seven Defendants Charged in \$2M Million Identity Theft and Credit Card Fraud Conspiracy," July 5, 2001.

<sup>8</sup>O'Connor, Matt and Michael Higgins, "U.S. says ID thieves used blood-donor list," *Chicago Tribune*, July 6, 2001.

<sup>9</sup>Prepared Statement of Al Schweitzer on the Use of Deceptive Practices to Gain Access to Personal Financial Information, before the Comm. on Banking and Financial Services, U.S. House of Representatives 105th Cong., 2d Sess., July 28, 1998.

<sup>10</sup>Federal Trade Commission Press Release: As Part of "Operation Detect Pretext" FTC Sues to Halt "Pretexting," [www.ftc.gov](http://www.ftc.gov), April 18, 2001.

<sup>11</sup>Prepared Statement of the Federal Trade Commission on H.R. 4311, the "Identity Theft Prevention Act," before Comm. On Banking and Financial Services, House of Representatives, 106th Cong., 2d Sess., September 13, 2000 (Statement by Betsy Broder).

<sup>12</sup>Hearing on H.R. 4311, the "Identity Theft Prevention Act" before Comm. On Banking and Financial Services, House of Representatives, 106th Cong., 2d Sess., September 13, 2000 (Statement by Janine Brenner, CALPIRG).

# FINDING SECURITY

in a

# GRAMM-LEACH-BLILEY WORLD

GERALD L. JENKINS

Adjunct Professor, John Marshall Law School—Center for Information Technology and Privacy Law Partner,  
Goldberg, Kohn, Bell, Rosenbloom & Moritz, Ltd., Chicago Illinois

*I*n a never-ending quest to serve customers, banks are embracing technologies that allow customers to do their banking when they want, where they want and how they want. Unfortunately, technology entails costs, as well as benefits. Costs include capital and operating expenditures, management resources and a variety of security risks.

Section 501(b) of the Financial Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act) was enacted by Congress to require financial institutions to evaluate the impact of security risks on their customers and to implement programs to control those risks. The Federal Reserve, FDIC, OCC and OTS have issued regulatory guidelines (the “Guidelines”) that are intended to help banks analyze and manage their customer information security risks. While banks should review the Guidelines carefully to meet statutory and regulatory requirements, they can also use the Guidelines as a cornerstone of an overall computer risk management program.

## BACKGROUND

Banks are no strangers to security risks and have historically taken the proper measures to defend against physical intrusions. However, thieves have still been attracted to banks despite the fact that the neighboring hardware store has weaker locks, no guards and no burglar alarms. Why? As Willie Sutton once said, “That’s where the money is.” If Willie Sutton were alive today and schooled in hacking techniques, he might well say the same thing about bank computer information systems. When faced with the choice between hacking a hardware store Web site with a few hundred credit card numbers and hacking into a bank, he would probably work much harder to breach the bank’s systems. In addition, if faced with the choice between robbing a bank the old fashioned way and hacking into a bank computer system, he might well abandon his hompson sub-machine gun in favor of a computer keyboard. Because banks constitute such a lucrative target for would-be computer criminals (who might be located anywhere on the planet), the security measures that a bank must take are significantly greater than the measures that the local hardware store would take. Just as a bank uses a vault when the hardware store finds a deadbolt lock sufficient, a bank may need a secure intrusion monitoring system when a firewall is good enough for the hardware store. It is against this backdrop that Congress decided to require financial institutions to implement a special set of security rules.

## THE STATUTORY LANGUAGE

Section 501(b) requires financial institutions to “establish appropriate standards...relating to administrative, technical, and physical safeguards” in order to:

- Ensure the security and confidentiality of customer information,
- Protect against any anticipated threats or hazards to the security or integrity of customer information, and
- Protect against unauthorized access to or use of customer information.

As important as safety and soundness issues are, Section 501(b) focuses on customer records and information. It should be noted, however, that many of the same security systems that protect customer information will also protect a bank’s other important data, and that a bank benefits if the knowledge and skills that it acquires protecting customer information is put to use elsewhere.

## THE GUIDELINES

The Guidelines require a bank to implement a comprehensive written information security program that includes administrative, technical and physical safeguards. The Guidelines do not mandate a specific set of safeguards. Instead they outline the process that a bank is required to undertake. The process is designed to help a bank determine what security measures it should implement based on its size and the complexity of its operations. The Guidelines provide the following multi-step procedure to develop, implement and maintain a written information security program:

A. *Assess the risk.* Assessing the risk involves:

- Identifying “reasonably foreseeable internal and external threats” that could compromise customer information.
- Assessing the damage that could result from the identified risks.
- Assessing the sufficiency of policies, procedures, information systems and other arrangements that are in place to control the identified risks.

Assessing risk involves far more than talking to a software vendor, installing a firewall and giving each customer a user name and a password. Because the majority of computer breaches are inside jobs that have nothing to do with Internet access, risk assessment is necessary even if a bank decides not to provide its customers with electronic banking services. External threats can come from rogue customers or from hackers who have no business relationship with the bank. Because risk or threat

assessment can be extraordinarily difficult, is often nonintuitive and typically depends on small details that may be unique to a particular bank, it is best left to people with expertise in security matters.

B. *Manage and control the risk.* Each bank shall:

- *Design its information security program to control the identified risks.* The bank should consider what controls, restrictions, procedures and other measures that it needs to provide. It should also analyze future computer system modifications to ensure that they are consistent with the bank's customer information security program.
- *Train staff to implement the information security program.* Staff training is often one of the most important features of a customer information security program. The most common method used by hackers to break into a computer system is called "social engineering" (analogous to pre-text calling). Social engineering is the use of persuasive techniques to convince bank staff to give out passwords and other key information that can be used to break into the bank's computer systems. For example, a male hacker may call the information services department saying that he is the husband of a trusted employee and that his wife is working on a mission-critical project, has forgotten her password and is unable to call herself. Without adequate training, many employees will fall for the ruse and readily divulge critical information.
- *Test regularly.* Testers should be independent third parties or staff members independent of those who develop and maintain bank security programs. Even though it may be difficult to convince staff to allow their handiwork to be tested by outsiders, it is even more difficult to create and maintain an effective information security program without testing.

C. *Oversee service provider arrangements.*

Each bank shall:

- *Exercise due diligence in selecting service providers.* Because information security is a difficult and highly technical discipline, choosing the correct service provider is an important decision. A bank should try to work with experienced service providers, check references and reserve the right to test the results on an ongoing basis.
- *Require service providers by contract to implement appropriate measures designed to meet the objectives of the Guidelines.* A bank should insist on contractual provisions that impose an appropriate level of responsibility on the service provider.
- *Monitor the service providers.* Not only should a bank insist on the right to monitor its service providers in its written contracts with them, but it should also implement internal programs to ensure that it takes advantage of its contractual rights.

D. *Adjust the security information program.*

Changing technology, changing sensitivity of customers about their information and changes to the bank and its information system will all require a reevaluation of the bank's information security system.

E. *Involve the board of directors and report to it annually.*

The board should oversee the customer information security system and assign responsibility for its implementation. The annual report to the board should describe the bank's compliance with the Guidelines and should address assessment, implementation, breaches and recommendation for change.

## **RISK MANAGEMENT ISSUES**

Security is an area where risk can never be totally eliminated. At best, security risks can be identified, measured and controlled. Without identification of real risks, time and money can be spent protecting against some, but not necessarily the most important, risks. A good example is a popular burglar alarm system that was installed in Beverly Hills a

few years ago. Nothing was left to chance. Every door and every window was wired to detect entry. Unfortunately, a crew of burglars went from house to house punching through walls with a simple battering ram. The burglaries would have been prevented with relatively inexpensive motion detectors. A systematic identification of risks before installation of the systems might have prevented the burglaries.

A bank should continuously monitor its computer systems. It might purchase a best-of-breed operating system and Web server, but if it does not keep track of known security holes and install the patches that plug those holes, it risks compromising its security. Typically proper ongoing management of systems is more important than the selection of the systems in the first place.

A bank should also implement effective intrusion detection and response. It should monitor activity on its systems and respond quickly to suspicious activity. A good analogy in the physical world is a safe. A safe is rated by how long it takes a safe-cracker to get access to its contents. A TL-30 safe is a safe that requires thirty minutes for a professional safecracker with tools to break in. A TLTR-60 is a safe that requires sixty minutes for a professional safecracker with tools and an acetylene torch to break in. Neither safe is particularly useful if it is not connected to an alarm or if the alarm does not lead to a response during the relevant time period. The same thing is true of a computer system. If, for example, a bank allows customers (and, therefore, hackers) to use an online system on a 24/7 basis, its intrusion monitoring system should be operational, and its intrusion response team should be ready to move quickly, both without regard to time of day or day of the week. Otherwise, a hacker can leisurely probe the bank's system, try to alter it and cover his tracks, all without fear of being caught.

A bank might also, as part of an overall risk management program, transfer risk through the purchase of insurance. Because an insurance company reviews a bank's information security program before it underwrites a policy, insurance will never

be a total solution. Insurance can, however, be an important part of an overall program that uses technology and training to control the risks and uses insurance to cover the cost of breaches that occur despite the controls in place.

Finally, as noted above, security risks can never be eliminated. They can only be controlled. Therefore, a bank should have a contingency plan to deal with the inevitable breach. Under what circumstances should an online system be shut down? How should customers who depend on the online system be informed? How should they be served in the interim? If new passwords must be issued, how can that be done quickly, cheaply and securely? Questions such as these should be addressed in a written crisis management plan.

The foregoing procedures will not only help a bank meet statutory and regulatory requirements, but they can also make the bank more secure across the board. Given the damage that a well-publicized breach can do to a bank's reputation and bottom line, no bank can afford to ignore them.



# ARTS IN ACTION

for

# AFFORDABLE HOUSING

JEREMIAH BOYLE

Community Affairs Program Director, Federal Reserve Bank of Chicago

**“T**oo many people in our tri-county community pay more than 30% of their income for housing and, in many instances, what they get for their money is sub-standard or even hazardous housing.” So says Dr. Michael Panhorst, Director of the Marshall Fredricks Sculpture Museum at Saginaw Valley State University (SVSU) in Michigan. Panhorst sees an opportunity for the university to be a collaborative partner with housing advocates and for his art students to lend their creativity to the effort to provide affordable housing in Saginaw, Midland and Bay counties.

So Panhorst created ShelterUS: Arts in Action for Affordable Housing. ShelterUS is a three-year collaboration between SVSU, Habitat for Humanity, East Shoreline Chapter of the American Red Cross, Midland County Affordable Housing Alliance, Created for Caring of Bay County, and Neighborhood Renewal Services of Saginaw. Chemical Bank & Trust and Bay Area Community Foundation are financial sponsors of ShelterUS.

In May, ShelterUS opened the “Designs for Decent Living” exhibition at the SVSU Art Gallery, as the centerpiece of their first year goal of creating awareness of the scope and nature of the affordable housing problem and getting more people involved. The goal of the exhibition is to stimulate discourse on the issues and facilitate collaborations that will help create more simple, decent housing in the tri-county area. A “sharing area” will provide space for non-profit housing advocates to publicize their services and successes such as profiles of Habitat for Humanity homeowner families, affordable housing developments and other educational materials. Chemical Bank created poster boards for the exhibit that explain mortgages and credit.

A conference table will enable small groups to meet in the gallery to address affordable housing issues while surrounded by images and information that illuminate the subject. The conference table itself is an interesting symbol of housing issues. Saginaw’s Habitat for Humanity salvaged seven doors from a house that is being demolished. Delta College woodworking students fabricated a round table with a hole in the middle from those seven doors. The hole in the middle is said to symbolize the

hole in the community created by a lack of affordable housing.

Designs for Decent Living, which runs through August 12, features innovative designs for affordable living such as “mail order” houses from Bay City in the early 20th century, Alden B. Dow’s “House with a Future” from mid-century and more recent innovations. Photographs of sub-standard housing and successful affordable housing projects in the tri-county area will also be included. In addition, artwork on the theme of shelter by SVSU art students will supplement the architectural images.

“We hope to open the eyes and minds of housing advocates to new and more economical ways to meet age-old needs,” said Dr. Panhorst. “The Designs for Decent Living exhibition is not an end in itself; its purpose is to stimulate creative thinking, dialogue and eventually, action on this pressing social issue.”

For more information on the exhibition and the ShelterUS collaboration, visit the ShelterUS web site at [www.svsu.edu/artgallery/shelterus](http://www.svsu.edu/artgallery/shelterus).



## BIOGRAPHIES

### Gerald L. Jenkins

*Adjunct Professor, John Marshall Law School—  
Center for Information Technology and Privacy  
Law Partner, Goldberg, Kohn, Bell, Black,  
Rosenbloom & Moritz, Ltd., Chicago, Illinois*

Gerald Jenkins serves as Adjunct Professor of Law at John Marshall Law School in its Center for Information Technology and Privacy Law. He teaches courses about security and privacy issues.

In addition, Mr. Jenkins leads the information technology and E-commerce groups at Goldberg, Kohn, Bell, Black, Rosenbloom & Moritz, Ltd., a Chicago law firm. He has drafted privacy policies for dotcom companies, educational institutions, as well as traditional bricks and mortar companies. He frequently speaks about privacy and security issues, including the impact of Gramm-Leach-Bliley on financial institutions and the Health Insurance Portability and Accountability Act on health care organizations. Mr. Jenkins has frequently spoken about privacy and security issues at the Federal Reserve Bank of Chicago seminars.

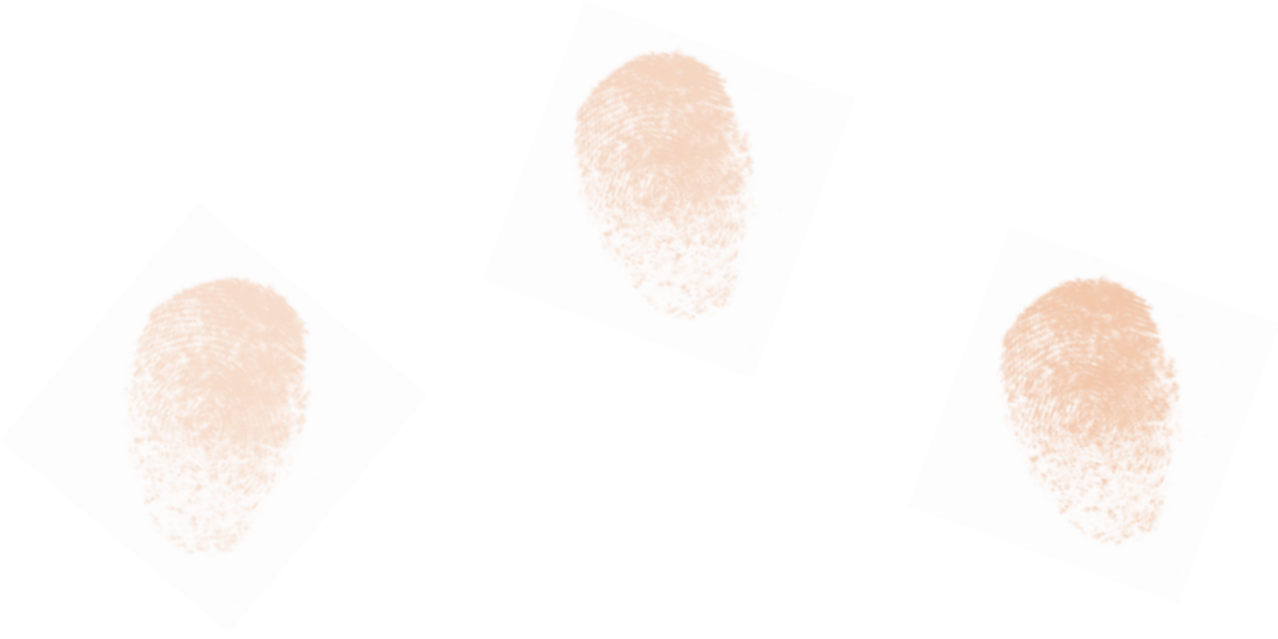
### John W. Connery

*Consumer Regulations Director,  
Federal Reserve Bank of Chicago, Chicago, Illinois*

John W. Connery is a Consumer Regulations Director with the Consumer and Community Affairs division of the Federal Reserve Bank of Chicago. He is responsible for researching emerging consumer compliance issues as well as providing technical assistance to member banks.

Prior to joining the Federal Reserve Bank of Chicago, Mr. Connery was an Assistant Vice President in the Compliance unit of ABN AMRO North America, Inc.'s Legal Department.

Prior to joining ABN AMRO, Mr. Connery was an examiner with the Office of Thrift Supervision. He was responsible for conducting compliance, CRA and trust examinations.



## Jeremiah P. Boyle

*Community Affairs Program Director,  
Federal Reserve Bank of Chicago, Chicago, Illinois*

Mr. Boyle is the Wisconsin Community Affairs Program Director in the Consumer and Community Affairs Division of the Federal Reserve Bank of Chicago. Mr. Boyle is the project coordinator for the Housing Opportunity Partnership for Southeast Wisconsin, Assistant Editor of (and contributor to) the Federal Reserve Bank of Chicago's Profitwise publication. Before joining the Fed, Mr. Boyle served as an Assistant Commissioner of Planning and Development at the City of Chicago; Economic Development Coordinator for the Village of Arlington Heights, Illinois; and several positions with the North River Commission, a nonprofit housing and economic development group in Chicago.

Mr. Boyle is a former director of the Chicago Association of Neighborhood Development Organizations (CANDO), and currently serves as a director of the North River Commission, the Peterson Park Improvement Association, and is a member of the North Park Village Advisory Council.

Mr. Boyle holds a certificate from the American Institute of Certified Planners, a Bachelor of Arts Degree in Political Science and a Masters Degree in Regional Planning from the University of Illinois at Urbana-Champaign, and a Master of Business Administration Degree from North Park University in Chicago.



**FEDERAL RESERVE BANK  
OF CHICAGO**

Consumer & Community Affairs Division

P.O. BOX 834

CHICAGO, ILLINOIS 60690-0834

**RETURN SERVICE REQUESTED**

*Attention:*

Executive Officers  
Board of Directors  
CRA Officer  
Community Lender  
Community Representative  
Compliance Officer

Profitwise is published by the Consumer  
& Community Affairs Division of the  
Federal Reserve Bank of Chicago  
230 S. LaSalle St.  
P.O. Box 834  
Chicago, IL 60690-0834

PRESORTED  
STANDARD  
U.S. POSTAGE PAID  
CHICAGO, IL  
PERMIT NO. 1942