

# FDIC

consumer news

Spring 1998

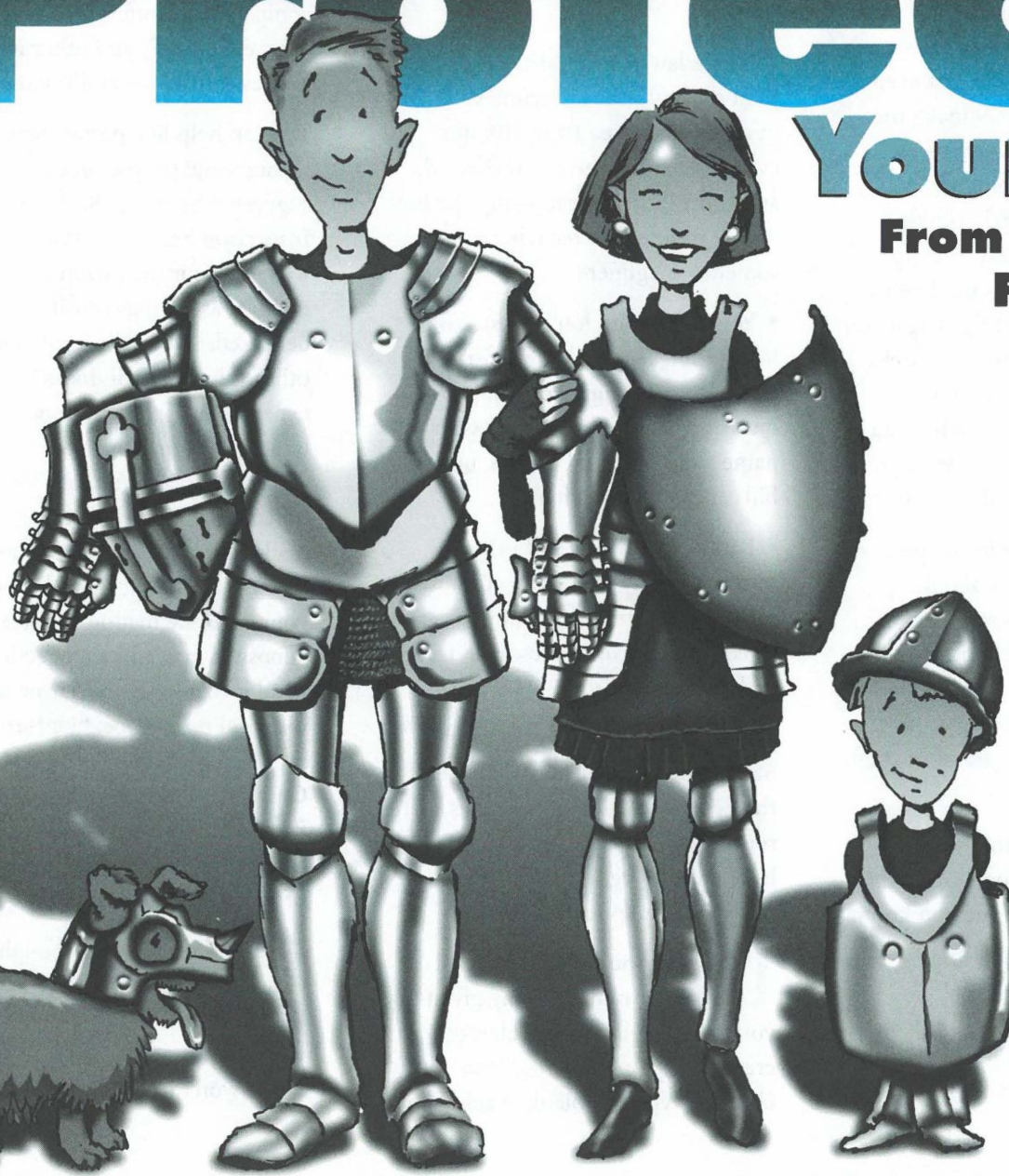
## Inside:

FDIC Deposit Insurance Simplified — Page 12  
New IRAs, New Insurance Determinations — Page 13  
Ways to Minimize ATM Fees — Page 14  
FDIC Plans Y2K Brochure for Consumers — Back Page

# You Can Protect Yourself From Financial Fraud and Theft

Our guide  
can help  
prepare  
you to  
battle  
fraud

Cover Illustration: T.W. Ballard





# You Can Protect Yourself From Financial Fraud and Theft

**Crooks and con artists have countless ways to rip you off, but you are your best anti-fraud weapon. Here's our guide to some of the best, easiest and most overlooked things you can do to protect yourself from financial scams and thefts.**

**W**e've all heard or read reports that a fraud or theft was stopped or some bad guy was apprehended because of an alert citizen. But even though the dramatic cases make the headlines, millions of "average people" are quietly helping to prevent or solve financial crimes, every day. You don't need to carry a badge or put your life on the line to make a difference in the fight against credit card fraud, counterfeit checks and other money-related offenses. You simply need to pay a little extra attention and take a little extra care as you go about your daily routine.

**FDIC Consumer News** in the past has run several warnings about specific types of crimes and how to guard against them. This time, though, we decided to print this special report on how to fend off practically any financial fraud or theft that may come your way.

We don't want to frighten you. If you're lucky, these crimes will never happen to you or someone you know. But we also think that crime prevention takes more than just luck — it takes knowledge and a willingness to take action, too. Here are some of the reasons we believe

you should take financial crimes seriously:

- While laws and industry practices limit dollar losses for crime victims in many cases (see Page 10), not everyone is 100 percent protected, and some end up swallowing the loss if they're found to have been somehow negligent.
- You may spend long, frustrating hours filling out police reports, closing old accounts, opening new ones and otherwise clearing your name from bounced checks, unpaid bills and other problems.
- Banks, merchants and other businesses may charge all consumers higher prices for goods and services to compensate for losses from fraud and theft.

So how can you protect yourself? Start by reading our list of some of the best and easiest approaches that, regrettably, too many consumers have either forgotten, dismissed or never even knew about.

**1 Protect your incoming and outgoing mail.** On any given day, your mail could include checks, credit card applications, "loan checks" (typically blank checks you

receive from your credit card company with offers to "write yourself a loan") and other items of interest to thieves and fraud artists.

You can help lick postal theft by taking some simple precautions suggested by the U.S. Postal Inspection Service in Washington: Remove your mail from your mailbox as soon as possible after it's delivered. If a check, credit card or other valuable mail doesn't arrive as expected or if the envelope appears tampered with, notify the sender and a postal inspector at your local post office. Also, never leave outgoing mail containing checks for utility or credit card bills at your doorway or your curbside mailbox. Instead, deposit it into a blue collection box, hand it to a letter carrier or take it to the local post office. "Unfortunately," says Ken Hunter, the Postal Service's Chief Inspector, "putting up the red flag on the curbside mailbox alerts thieves that there may be something of value to steal."

We add the following thoughts: Consider having your pay and benefit checks directly deposited into your bank account. That way your check won't get lost or stolen in the



mail or at home. Also, for checks you write regularly, perhaps for your mortgage or an investment into a mutual fund, think about having the funds automatically deducted and transferred directly by your bank. "Not only are electronic transfers safer and quicker than written checks, but problems or mistakes can be more easily tracked and resolved," says Alan Cox, an FDIC consumer affairs specialist in Washington. He explains that when an error in an electronic transfer is brought to a bank's attention, "it's required by law to investigate the matter promptly."

If you want to cut back on mailings of loan or credit card offers, there are several ways to do that (many are described in our winter issue, which is available from the FDIC's Public Information Center or our Internet site, both listed at right). Finally, if you're concerned about the security of your mailbox, consider putting a mail slot in your door or renting a P.O. box.

## 2 Stop thieves from turning garbage bins into gold mines.

Fraud artists know how to recycle trash into cash. How? So-called "dumpster divers" pick through rubbish and find things they can use to counterfeit or order new checks or credit cards. "That old saying about 'one man's trash is another man's treasure' is certainly true in this case," says Gene Seitz, a fraud examiner with the FDIC in Washington. So the next time you want to get rid of credit card receipts or applications, old credit cards, canceled checks, monthly statements or loan checks, tear them up into bits before you put them in the trash. You might even want to scatter the pieces into separate trash bins.

For similar reasons, always take your receipts and carbons with you after using plastic at an ATM, gas station, store, restaurant or anywhere else. Take them home and keep them in a safe place, at least long enough to make sure your account statements are correct. Then when it comes time to dispose of them, do it the safe way — slice 'em and dice 'em first.

## 3 Be extra careful with the checks, credit cards, debit cards, ATM cards or similar banking items you carry around.

Many people think it's no big deal to leave their wallet unattended, even just for a few minutes, inside their car, office or gym locker, or at a store, restaurant, phone booth or other public place. Unfortunately, wallets and their contents are easy to lose or have stolen. As we've said in the past, never set down your wallet in public unless your hand is attached to it.

Also, don't carry around more blank checks than you really need, just in case you lose your wallet. Likewise, consider canceling any credit cards you don't really need or use, because they're still valuable to a thief.

## 4 Closely protect your Social Security number, bank account numbers and other personal information.

If you think a crook needs to steal an actual check or bank card to commit a crime, think again. Just knowing your credit card account number and a little personal information about you (such as your Social Security number, birth date, address or your mother's maiden name) can be enough for a con artist to make or order new cards

*continued on next page*

## FDIC Consumer News

*FDIC Consumer News* is published by the Federal Deposit Insurance Corporation

**Donna A. Tanoue**  
*Chairman*

**Phil Battey**  
*Director*  
Office of Corporate Communications

**Elizabeth Ford**  
*Assistant Director*  
Office of Corporate Communications

**Jay Rosenstein**  
*Senior Writer-Editor*

**Tommy Ballard**  
*Graphic Design and Illustration*

*FDIC Consumer News* is produced by the Office of Corporate Communications, in cooperation with other FDIC Divisions and Offices. It is intended to present information in a nontechnical way and is not intended to be a legal interpretation of FDIC regulations and policies. Mention of a product, service or company does not constitute an endorsement. This newsletter may be reprinted in whole or in part. Please credit material used to *FDIC Consumer News*.

Comments, suggestions or questions may be sent to:

Jay Rosenstein  
FDIC, 550 17th Street, NW,  
Washington, DC 20429  
Internet: [jrostein@fdic.gov](mailto:jrostein@fdic.gov)  
Fax: (202) 898-3870

## Subscriptions

Subscriptions to *FDIC Consumer News* are available free of charge. Send subscription requests and address changes to:

FDIC, Public Information Center,  
801 17th Street, NW, Room 100,  
Washington, DC 20434  
Phone: (800) 276-6003 or  
(202) 416-6940  
Internet: [publicinfo@fdic.gov](mailto:publicinfo@fdic.gov)  
Fax: (202) 416-2076

## On the Internet

*FDIC Consumer News* and other consumer information from the FDIC is available on the Internet via the agency's home page ([www.fdic.gov](http://www.fdic.gov)).



in your name, or to simply buy goods and services over the phone.

Here are a few ways to keep this information from criminals. First, never give your credit card number, Social Security number or other personal information to anyone over the phone unless you make the call to someone you know and trust. Never divulge this kind of confidential information to a telemarketer who calls your house. Also never give this information to a caller who claims to represent your credit card company, warns Randy Schoultz, a fraud specialist with the FDIC in Memphis. "Tell the person you'll call back and be sure to use the customer service phone number on your credit card," he says.

Don't have your Social Security number pre-printed on your checks. And don't carry personal identification numbers (PINs) for your ATM card or credit card in your wallet; try to memorize them instead.

**5 Thoroughly check out any unsolicited offer before agreeing to anything.** Swindlers often pose as legitimate business people, charity workers or law enforcement officers just to convince people to give up cash, checks, credit card numbers and other valuable information. Unfortunately, too many people fall for a friendly voice, an official-looking document and a fantastic-sounding sales pitch that's really part of a scam.


We suggest you walk away or hang up if... you get an unsolicited offer that sounds too good to be true... you're being pressed to say yes immediately... and you're asked to give money or bank account information before you can receive

anything in return. These are classic warning signs of a fraud. Before saying yes to any offer, ask for details in writing and research the matter carefully. If a lot of money is involved, you also might want to check out the organization with the Better Business Bureau, the police, or your state's Attorney General or consumer protection office.

**6 Closely review your credit card bills and bank statements.** Open this mail as soon as possible after it arrives to make sure that no one else is using your account and to protect yourself from claims that you were in some way negligent (especially important with checking and savings accounts). Compare the list of transactions with your own records and receipts, and generally search for anything that may be questionable. And if your credit card bill or monthly bank statement doesn't arrive as expected, that could be a sign that someone has stolen this important mail or put in a fake change of address as part of a fraud scheme. Call the issuer immediately.

It's also a good idea to periodically review your credit reports, maybe once a year or so, to make sure someone else hasn't used your name to get a credit card or a loan. For a copy of your credit report from the three major credit bureaus, call these special toll-free numbers: Equifax at (800) 685-1111, Experian at (800) 682-7654, and Trans Union at (800) 888-4213. Under 1996 amendments to the Fair Credit Reporting Act, the most you can be charged for your credit report is \$8, but you're entitled to a free copy once a year under certain circumstances (including if you've been a fraud victim).

## Final Thoughts

We've tried to point out some of the best, simplest self-protection techniques that you can use in your daily affairs. Now keep reading to find even more ways. We can't say that if you follow our advice you'll never be a victim. We also can't guarantee you'll ever make headlines as a crime fighter. But we do think you'll make headway in the efforts to make our neighborhoods and our financial services safer and more secure. 

## Who to Call to Report a Financial Crime

If you think you're a victim of a financial crime or if you notice anything suspicious, get to the phone right away and call the following:

- The police.
- Your bank, credit card company or other financial institution that may need to know about the matter.
- The National Fraud Information Center (800-876-7060, Internet site [www.fraud.org](http://www.fraud.org)), which forwards reports of suspected fraud to federal and state authorities.

Also, consider calling the three major credit bureaus. Ask them to place a fraud notice in your file, so that lenders and other users of credit reports will be warned to be careful before approving a new credit card in your name. Two of the three credit bureaus publicize the toll-free numbers for their fraud department: Experian at (800) 301-7195 and Trans Union at (800) 680-7289. Equifax asks that you first contact your creditor or the police in order to get the phone number for its fraud unit.



## Classic Cons... and How to Counter Them

### A laundry list of dirty tricks used by fraud artists

#### ATM Theft

**How it works:** Automated teller machine (ATM) crimes can take several forms. Thugs may simply approach someone using an ATM and demand money. Or, more sophisticated thieves will watch the victim use the card (perhaps even with high-powered binoculars) and learn his or her card number and personal identification number (PIN). Later they'll steal the card or make their own and go back to ATMs for cash.

**Warning signs:** One or more persons loitering around the ATM, often in a car, behind bushes or otherwise nearby. You spot unauthorized ATM withdrawals on your bank statement.

**Best defense:** Use only ATMs in well-lit, busy areas where unusual activity would be noticed. For after hours or late night use, the best choice may be an ATM in a supermarket, convenience store, gas station or other protected area. When in doubt about a particular location, go on to another ATM where you'd feel safer.

#### Check Fraud

**How it works:** Someone steals checks from your home, office or mailbox and forges your signature. Crooks don't need blank checks to pull off a check fraud. Many know how to easily remove the ink on checks, often by "washing" them with a cleaning solvent. They also will alter what's already been written, such as by changing a check payable to the I.R.S. to one payable to J.R. Smith. A counterfeiter also can make new

checks in your name using a home computer and a printer.

**Warning signs:** You notice that checks are missing from your checkbook or your reserve supply of checks. Mail containing checks or bank account information is "lost" or appears to have been tampered with. You spot unauthorized transactions on your bank statement.

**Best defense:** Don't carry more checks than you need. Keep extra checks in a secure place. Write checks using a pen with thick, dark ink. Draw lines to fill in gaps in the spaces where you designate to whom a check is payable and the amount. John Brugger, a U.S. Postal Inspector in Washington, adds that consumers should "insist that their checks have built-in security features that help make them tamper-resistant to check washing or counterfeiting." Also immediately report to your bank any irregularities in your bank statements. Report mail theft or tampering to the U.S. Postal Inspection Service, which is listed in your phone book.

#### Credit Card Fraud

**How it works:** There are hundreds of ways. Here are just a few. A thief may steal your credit card. Someone may order a new credit card in your name by stealing a pre-approved application from your mail and having the card sent to a different address. An unscrupulous sales clerk can make a duplicate copy of your credit card receipt or use a special device to capture data from the magnetic stripe on your card. One

way or another, the thief using phony ID can make or order a credit card, in your name, and use it to obtain merchandise or cash advances.

**Warning signs:** Unauthorized charges appear on your credit card statement or you get a statement for a credit card you didn't request. Your mail appears to have been tampered with. Mail containing a new credit card or a credit card statement doesn't arrive as expected.

**Best defense:** Promptly report to the card issuer any unusual activity on your statement. If you receive a card you never asked for, or if you don't get a card you're expecting, promptly report that to the issuer. Protect your credit cards and card numbers, and don't keep PIN numbers near the cards. Properly destroy all credit card receipts and statements when no longer needed. Limit the number of credit cards by canceling those you don't use. Cut up old cards after they expire.

#### Debt Relief Fraud

**How it works:** Several frauds and rip-offs are targeting people having debt problems. Some ads declare that a bad credit history can be "erased" or that "debt consolidation" can quickly cure credit problems. Most often, the consumer will pay exorbitant fees or interest rates for unnecessary services. Other ads tout easy ways consumers and small businesses can get low-cost loans, often even without a credit check or collateral. But in many cases the up-front fees are excessive or never lead to a loan

*continued on next page*



being given. Some unscrupulous lenders also may offer to “consolidate” your loans into one loan with no credit check. These may turn out to be home equity loans that carry exorbitant interest rates, onerous payment terms, and the risk of foreclosure on the consumer’s home.

**Warning signs:** Many legitimate lenders provide debt consolidation loans, but you should shy away from offers that promise to erase a bad credit record if you simply pay a fee and combine different debts into one new loan. Only years of steady performance in paying debts can repair a credit history. Be wary of anyone offering to erase your bad credit record by creating a new identity for you, perhaps by ordering a new Social Security number. That’s illegal. Beware of anyone who asks for money up-front to “guarantee” approval of a loan. “Advance fees” should not be confused with application fees charged by many legitimate lenders, who do not “guarantee” approval of loans after receiving an application fee. Also beware of people who hold seminars to sell kits they say can be used to pay off your mortgage or other debts. The kits, which typically cost \$300 to \$500, contain items that look like checks but have names like “certified drafts.” Purchasers are told the drafts can be issued in any amount. In reality, these items are worthless, and anyone who pays bills with them risks being prosecuted for using a fraudulent instrument.

**Best defense:** If you have credit problems, immediately contact your banker and other creditors. Don’t wait until your accounts are turned over to a debt collector. Most of the time, creditors will work with you on

a solution, especially if you’ve had a good record in the past. If you can’t solve your debt problems on your own or with the help of lenders, there are other reliable sources of help, including state and local agencies that also offer credit-counseling services for little or no charge. One way to re-establish credit is by obtaining a “secured” credit card (you post a deposit that’s usually equal to or greater than your credit limit) and make your payments on time for a year or so. Not all secured credit cards carry the same interest rates and terms, so shop around. Before agreeing to any loan, deal only with reputable lenders, read the fine print, compare interest rates and question any unusual fees.

### Fraudulent CDs

**How it works:** You see a newspaper or Internet advertisement by an unknown bank, probably one far away, claiming to offer insured certificates of deposit (CDs) at unusually high interest rates. The ad also may say the funds will be held in accounts in “tax haven” countries where the interest will be free from U.S. taxes and protected from scrutiny by U.S. authorities. You send in your money only to learn

later that the bank is bogus and the CD is not federally insured. Chances are you won’t see your money again.

**Warning signs:** The most obvious sign is an extremely high interest rate compared to market rates for CDs advertised by reputable institutions. To fool unsuspecting investors, many successful scams also have involved so-called banks with names very similar to large, well-known U.S. banks. Some foreign entities also say they have “private” insurance for your investment, but this may just be a false claim made only to soothe the fears of potential depositors.

**Best defense:** As with any deposit or investment, check things out and know who you’re dealing with before sending money. Crooks can counterfeit CDs as easily as checks, so if you want the security of a federally insured CD, only buy from a federally insured financial institution or a reputable broker. Some con artists call themselves banks and falsely advertise FDIC membership to fool unsuspecting depositors. You can find out if an institution is FDIC-insured by contacting the FDIC’s Division of Compliance and Consumer Affairs (see Page 15) or doing research on

### New FDIC Program to Help Consumers Avoid and Report Fraudulent Internet Banks

As we’ve warned elsewhere in this issue and in previous editions of our newsletter, unscrupulous people and groups establish Internet sites that claim to be insured banks when, in fact, they don’t have a legitimate banking charter and are not FDIC-insured. Consumers who send money to a bogus bank run the risk of losing their funds. To help get these sites off the ‘Net, the FDIC is developing a new

service on our Internet home page ([www.fdic.gov](http://www.fdic.gov)) that will enable consumers to check the validity of a bank Web site (before they do business) and to report suspicious new sites via an e-mail to the FDIC. The system is expected to be up and running soon, so watch for more details in an upcoming **FDIC Consumer News** and on the FDIC home page.



the FDIC's Internet site ([www.fdic.gov](http://www.fdic.gov)). Also check out the box at the bottom of Page 6 about the new FDIC program aimed at fraudulent Internet banks. And remember that deposit brokers may sell FDIC-insured CDs, but the brokers themselves are not insured by the FDIC. If you're not familiar with the broker, contact the Securities and Exchange Commission (SEC) or your state securities regulator.

## Identity Theft

**How it works:** By trickery or using publicly available information, someone obtains personal information about you, assumes your identity and applies for credit cards or checking accounts. The crook has become "you." He or she then can go on a spending spree.

**Warning signs:** You get bills, credit card statements, calls from businesses or collection agencies, or other notices for debts and purchases you know nothing about.

**Best defense:** Don't give credit card numbers, Social Security numbers or other personal identifying information to anyone over the phone unless you initiate the call. Legitimate banks and others who offer credit cards, such as telephone companies, *never* call customers asking for information such as PIN numbers. Don't include your Social Security number on your checks. Protect your mail and your trash from financial thieves (see Pages 2 and 3). If you become aware of anyone using your identity, immediately notify the creditor, law enforcement authorities and the major credit bureaus.

## Internet Fraud

**How it works:** Unusual or inexpensive goods and services are offered over the Internet. The consumer typically pays for something that doesn't arrive, or the goods and services are not as advertised.

**Warning signs:** Exaggerated claims often aren't easy to spot, but if something sounds too good to be true, it probably is a scam. Although people selling goods and services over the Internet may claim lower overhead by selling directly to the public, you should use common sense in determining whether their claims are reasonable. For instance, if a bank doing business over the Internet offers 20 percent interest on deposits, is their cost of business so much less that they can quadruple the interest rate paid by traditional banks? Most likely, it isn't.

**Best defense:** When banking or buying over the Internet, only give credit card or other personal information to companies you know and trust. If you don't know anything about the company, contact your local Better Business Bureau to find out if any complaints have been filed. Your Internet service provider also can provide useful advice about safely using the 'Net. Also see our warning about fraudulent CDs on the previous page. For more tips for avoiding online problems and scams, see the fall 1997 issue of *FDIC Consumer News*.

## Investment Fraud

**How it works:** You get or see an offer of "guaranteed" big returns (up to 100 percent or more) on investments, business opportunities and other "no-risk" deals. Many of these deals

involve pyramid schemes where funds received from new investors are used to pay earlier investors, thus lending credibility to scam artists who may boast of returns paid to investors. At some point, though, the crook takes the money, flees the area, and leaves the latest investors with nothing but worthless paper. A related scam involves "prime bank" instruments. These are nonexistent investments that scam artists advertise as returning 100 to 1,000 percent of the investor's original investment.

**Warning signs:** Avoid investments that defy logic and offer unrealistic

*continued on next page*

## Federal Agencies Help Protect Crime Victims, Witnesses

Victims and witnesses of white collar crimes have rights under federal law to ensure that they are treated fairly during investigations and trials and that they are reasonably protected from threats and harassment. The FDIC and other federal and state law enforcement agencies have services and educational materials that they provide to help crime victims and witnesses deal with the anger, confusion, frustration or fears they may have as a result of their experience. For more information about victim and witness assistance programs, contact an appropriate law enforcement agency. For information from the FDIC, write to the Office of Inspector General, 801 17th Street, NW, Washington, DC 20434.



returns. Again, if it sounds too good to be true, it probably is a scam. Avoid high-pressure sales pitches. "If these supposedly high-return, no-risk investments were legitimate, nobody would have to contact you or pay to advertise them," says Gene Seitz, an FDIC fraud investigator based in Washington. "They wouldn't even have time to call you because they'd be too busy answering incoming calls."

**Best defense:** Deal only with reputable investment firms. Ask the SEC or your state securities regulator about the legitimacy of a broker or an investment opportunity. Check out business opportunities with places such as your state corporation licensing division and/or the Better Business Bureau.

### Nigerian Scam

**How it works:** You receive an official-looking letter from someone claiming to be a Nigerian who, because of Nigerian government rules, needs help transferring money out of that country. Perhaps you're asked to deposit the funds into your bank account for a "reward" of 20 to 30 percent of the funds, which usually are in the millions of dollars. To do your part, you're simply asked

to supply your bank account number and some money supposedly to cover "expenses." But the crooks behind these scams simply keep your money and use the account information to steal more money. Another variation involves a request that you act as a "front" in a real estate purchase so the true identity of the Nigerian can be kept secret. You're offered a hefty fee for your services but you'll have to provide "good faith" money and help pay certain expenses. Then the only funds exchanged go from the unsuspecting victim to the con artist.

**Warning signs:** Nobody is going to give you a percentage of millions of dollars simply for the privilege of using your bank account or your name to transfer money to the U.S. Some people have lost their lives trying to collect their money lost in this scheme.

**Best defense:** If you receive a letter or fax containing promises of instant wealth, don't respond. Promptly take it to your nearest U.S. Postal Inspection Office.

### The Phony Investigator

**How it works:** A consumer, often an elderly person, is approached by

someone claiming to be a bank examiner, bank security officer, police officer, Internal Revenue Service (IRS) auditor or some other "agent" involved in an "official" review or investigation. For example, the consumer may be asked to withdraw cash from his or her bank account, or to let the investigator review personal account records, supposedly to aid in an investigation of a possible fraud at the bank. The successful con artist walks away with the cash or the confidential information that can be used to raid the consumer's bank account.

**Warning signs:** Be wary of anyone who approaches you claiming to be a government employee investigating a bank, a bank employee, or otherwise asking for access to your cash or bank records. Government agencies do not turn to bank customers to withdraw personal funds or give account information as part of an investigation. Also, in cases such as IRS audits, you'll be notified in advance by mail.

**Best defense:** Decline any requests to give cash or confidential information to anyone who approaches you claiming to be a police officer or government investigator. Promptly

## Have a Safe Trip

Follow this roadmap to trouble-free travel, whether you're going on a business trip or vacation

- Don't take along a lot of cash. Consider using traveler's checks, ATMs and credit cards.
- Don't flaunt your cash, charge cards, jewelry, passport, etc.
- At hotels and motels, consider keeping jewelry and other valuables in a safe.
- Report a lost or stolen credit card immediately to limit your liability for unauthorized charges by a thief.
- At airports, be on guard against thieves who target weary travelers (and their cash, credit cards and other belongings).
- Carry a list of toll-free phone numbers for your bank and credit card companies, so you can report a lost item and get replacement cards or cash. Don't list your account numbers, your Social Security number, PIN or other confidential numbers.
- Ask a "guardian angel" back home — a trusted friend or neighbor — to pick up your mail and keep an eye on your house. Leave a copy of your itinerary so you can be reached in an emergency.




report the matter to your bank's security officer and/or local law enforcement authorities.

## Telemarketing Fraud

**How it works:** You get an unsolicited phone call or mailing with an offer of prizes, a vacation package, merchandise or other opportunities that are said to be "too good to miss" and "available only if you act now." You agree over the phone to give cash or bank account information up-front to take care of a supposedly minor fee or tax. Later you discover that the con artists have taken your money and you have little or nothing to show for it.

**Warning signs:** High-pressure sales people offer prizes, goods or services that can only be delivered upon receipt of cash, a credit card number or checking account number. While prizes are usually subject to federal income taxes, this money is only payable to the IRS when you complete your income tax returns. Taxes never are collected up-front when legitimate prizes are awarded. Be wary if the caller says merchandise is "unique" and available only at a special price if purchased now.

**Best defense:** Buy only from a reputable telemarketing firm. Never pay a fee to receive something "free." If you have doubts about a particular firm, contact the Better Business Bureau and/or the Federal Trade Commission to see if complaints have been registered against the firm. Also keep in mind that seemingly innocent "telephone surveys" may be used by scam artists to collect information that can be used in future telemarketing frauds. 

## Subtle Signs of a Swindle

To learn how to avoid a crime, you talk to crime victims, right? Not always, says psychology professor Monroe Friedman, who studies financial crimes against seniors. That's why he believes many educational materials from law enforcement and consumer protection agencies have one big limitation. "They're often based on the actual stories of fraud victims — of people who, when accosted by a scamster, failed to detect a red flag or didn't know how to escape from the situation," he tells FDIC Consumer News. "I decided to look at the people who avoided becoming victims — the successes, not the failures. That shows a very different picture of how people cope."

Friedman, a researcher at Eastern Michigan University in Ypsilanti, used a grant from the AARP Andrus Foundation to study 304 older people who sidestepped financial swindles. His most recent analysis, reported in the summer 1998 edition of the scholarly "Journal of Consumer Affairs," shows that it sometimes pays for consumers to look for a combination of small, subtle danger signals — not just one or two concrete developments (such as a request from a stranger for your credit card number).

"It might be something fishy early in a conversation that makes you leery, then later something else, that in combination make you say, 'I smell a rat,'" he adds in our interview. "People who are successful in avoiding a fraud often look at these bits and pieces and, once they add it all up, decide to say no to a questionable offer."

These are some of the 25 danger signals Friedman's psychological research identified and that, in combination, should make a consumer suspicious of an offer:

- You're told you've been specially selected for an offer or that you previously accepted an offer and you know you hadn't.
- The person was "more friendly" than seemed appropriate given that he or she didn't know you.
- The suspect said something you knew or thought wasn't true.
- The conversation appears to be "high pressure" or intimidating.
- The method of contact (mail, phone or in-person) seems inappropriate for the kind of offer being made.

Friedman gives this example from his research: A person in Boston is approached by a young woman selling magazines, supposedly to earn enough money so she can realize her lifelong dream of going to college. When asked which college she plans to attend she responds, "The University of Boston." What's the problem here? "If you live in Boston, you know that's not the name of the school; it's just not something a local person would say," says Friedman. "That one answer wasn't enough to shut the situation down, but it was enough to raise questions." And that, together with other danger signals, ended the conversation before a fraud was committed.

*Are you a success story or do you know someone who is? See Page 11.*



## A Crook Has Drained Your Account. Who Pays?

Federal laws and other protections may limit your losses if you fall victim to a bank fraud or theft

**A** swindler runs up a big bill on your credit card or steals hundreds of dollars from your bank account. Do you suffer the loss? In many cases of bank crimes, your liability is limited by law or industry practices to the first \$50 of loss, but that depends on the type of account and how quickly you report the problem.

Suppose a thief obtains your **ATM card** and uses it at an automated teller machine to withdraw money from your bank account. Under the Electronic Funds Transfer Act, your losses are limited to \$50 if you report your ATM card lost or stolen within two business days of discovering the loss. If you wait between two and 60 days of discovering the loss, you can be liable for up to \$500 of what a thief withdraws. If you wait more than 60 days after receiving a bank statement that includes an

unauthorized transfer, the law doesn't require your bank to reimburse you for any losses. You're not responsible, however, for any funds withdrawn after you notify your bank that the ATM card is lost or stolen.

What if your **credit card** is lost or stolen and gets used by a thief? Under the Fair Credit Billing Act, your losses are limited to \$50 per card. As with ATM cards, you're not responsible for charges made after you report the card lost or stolen.

More and more people are using **debit cards** (or "check cards") to pay for purchases from a checking account without writing a check. By law, a consumer's liability for an unauthorized use of a debit card is comparable to that for an ATM card, which may be far higher than that for a credit card (\$50 maximum loss). However, it's easier for a thief to deplete an account with a debit card than with an ATM card, because some debit cards require only a signature, not a personal identification number (PIN). Fortunately for consumers, though, VISA and MasterCard have voluntarily limited debit card liability to the same \$50 limit that exists for credit cards.

The **stored-value card** has emerged in recent years as another way to purchase items. These cards are purchased with cash and have a fixed value that gets reduced as purchases are made at merchants that accept the card. If a stored-value card is lost or stolen, it's like losing cash, and no

federal law protects you.

While no federal law limits your losses if someone steals your **checks** and forges your signature, you do have protections under state law. Most states hold the bank responsible for losses from a forged check. However, most states also require the customer to take reasonable care of his or her account. You may be held liable for the forgery if you don't notify the bank in a timely manner that a check was lost or stolen, or if you don't monitor your account statements and promptly report an unauthorized transaction. Pay attention to your accounts. Contact your state's consumer protection office to learn more about your rights.

Many banks also purchase a form of insurance called a banker's blanket bond that may protect them from robbery, burglary, embezzlement and other causes of disappearing funds. The banker's blanket bond would cover the bank and, most likely, ensure that funds taken from your account would be covered.

Finally, your credit history can receive unfair blemishes when a thief uses your credit card, debit card or checking account. But under the Fair Credit Reporting Act, if you think your file contains incorrect information you're entitled to an investigation by the credit bureau. If you disagree with the results, you have the right to include in your credit file a brief statement giving your side of the story. 🏠

### What is FDIC-Insured?

Many consumers mistakenly assume that FDIC insurance must protect them from a fraud or theft if the funds were taken from an insured account. But by law, deposit insurance only protects your accounts up to \$100,000 if your insured bank or savings institution fails. To learn more about what is and is not protected by FDIC insurance, read our brochure "Insured Or Not Insured," which is available free of charge from our Public Information Center (Page 3) or on the Internet ([www.fdic.gov/consumer/fdiciorn.html](http://www.fdic.gov/consumer/fdiciorn.html)).



## He's Not From the Government... and He's Not Going to Help You


**G**overnment agencies work hard to serve the American people and earn your trust. Unfortunately, there are unscrupulous people and companies who try to take advantage of this trust — and take advantage of consumers — by tricking them into thinking they're dealing with legitimate government officials. We want you to beware of scams, deceptive marketing campaigns or otherwise questionable activities that trade on the government's good name and reputation. They include:

- **Charging a fee for services that are available free from the government.** Common schemes involve writing or calling with claims of inside information and offers to help recover unclaimed property or get a refund from the government, for a fee, when all of that can be done at no charge by dealing directly with the agency involved.
- **Getting up-front payments for bogus offers.** The files of the FDIC's Office of Inspector General

include the case of a Texas motorcycle dealer who was convicted for persuading people to invest millions in FDIC-owned luxury automobiles and corporate airplanes that did not exist. Other cases involve convictions against imposters who convinced home buyers to send them big down payments for special deals on real estate supposedly owned by the government.

• **Falsely claiming that goods or services are approved or backed by a government agency.** Two examples — phony banks that falsely advertise themselves as FDIC-insured and crooks who pretend to be bank examiners — are described in our listing that begins on Page 5.

One way companies dupe consumers is by using a name or acronym that leads people to believe they are dealing with a government agency (although there are many legitimate and law-abiding companies or organizations with names similar to a government agency).

How can you protect yourself? Beware of unsolicited offers for deals that seem too good to be true and from a person or company claiming or appearing to be from the government. When in doubt, go to your phone book or another directory of government agencies and call to confirm the validity of the offer. Don't trust the phone number given to you otherwise. That could be part of the scam. Also consider contacting your state government (the consumer affairs office or attorney general listed in your phone book), the local Better Business Bureau (also in your phone book) or the Federal Trade Commission's Consumer Response Center (6th & Pennsylvania Avenue, NW, Washington, DC 20580, phone 202-326-3128 or e-mail [consumerline@ftc.gov](mailto:consumerline@ftc.gov)). If you're suspicious about someone claiming to represent the FDIC, call our Office of Inspector General toll-free at (800) 833-3310. 

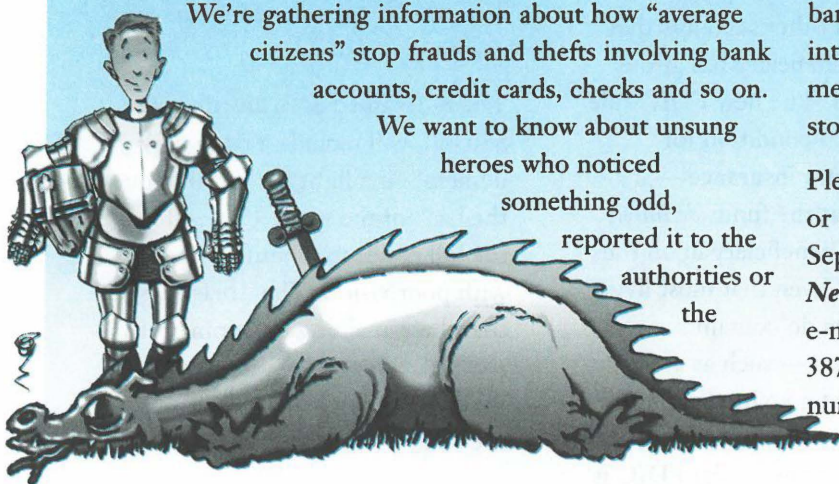
## Calling All Crime Solvers: Tell Us Your Stories

We're gathering information about how "average citizens" stop frauds and thefts involving bank accounts, credit cards, checks and so on.

We want to know about unsung heroes who noticed something odd, reported it to the authorities or the

bank, and learned later that a crime was thwarted. We're also interested in any additional crime-fighting tips not mentioned in this issue of *FDIC Consumer News*. The best stories and suggestions may appear in a future issue.

Please send your stories (including any newspaper clippings or other supporting material) and your words of wisdom by September 1, 1998 to: Jay Rosenstein, *FDIC Consumer News*, 550 17th Street, NW, Washington, DC 20429. The e-mail address is [jrosenstein@fdic.gov](mailto:jrosenstein@fdic.gov). Our fax is (202) 898-3870. Please also include your name, address and phone number. No names will appear in print without permission.





# Deposit Insurance: Simpler is Better

## The FDIC clarifies the rules for the benefit of consumers and bankers

**T**he FDIC knows that the deposit insurance rules can be confusing—for consumers and for bankers—and that's a concern for everyone. Why? "When an insured institution fails, this confusion can mean, in some cases, a substantial loss of funds for depositors who think that they are fully insured but discover too late that they are at least partly uninsured," says Chris Hencke, an attorney in the FDIC's Legal Division in Washington.

To help solve this problem, the FDIC Board of Directors recently adopted changes that will make the rules easier to understand. The major change inserts into the rules a variety of straightforward examples that will help a depositor read the rules and quickly understand the scope of insurance coverage at an FDIC-insured bank or thrift.


The FDIC also adopted three substantive changes that:

- **Provide a six-month grace period after a depositor's death for the survivors to rearrange the accounts if necessary to avoid going over the \$100,000 insurance limit.** Grieving families often need time to put their affairs in order after a death. But under existing rules, for example, a joint account for a husband and wife likely would *automatically* become the surviving spouse's money when the other dies. That alone could put some of the survivor's insurance coverage over the \$100,000 limit. To reduce the chances this might occur, the FDIC is adding the grace period.

- **Give the FDIC more flexibility to insure deposits made by agents (such as escrow companies or title companies) on behalf of their customers.** Money from the sale of your home may be temporarily deposited by a real estate agent in an escrow account he or she maintains at a bank, perhaps for you and other clients, too. If the bank's records clearly indicate that the agent's account is for several clients, the account would be insured to \$100,000 for each client, not just to \$100,000 in total. The new rule makes it easier for the FDIC to reach that conclusion in the absence of clear records on file at the bank.

- **Warn owners and beneficiaries of a "living trust account" about conditions that might limit the insurance coverage of the account.** A living trust account is a type of payable-on-death (POD) account opened in connection with a formal trust agreement that the owner can cancel or change during his or her lifetime. If certain conditions are met, the share of each beneficiary in a POD account qualifies for \$100,000 of insurance separate from the coverage on other accounts that the owner or beneficiary has at the same institution. The new FDIC rule clarifies one such condition for receiving the extra insurance — a requirement that the funds *definitely* will pass to the beneficiary upon the owner's death. Given that most living trust agreements do contain restrictive clauses — such as a requirement that a young beneficiary graduate from college before inheriting the money — the FDIC is

warning people who set up living trusts to be aware of the insurance implications. Living trust accounts with these kinds of strings attached will be combined with the owner's individual accounts for up to \$100,000 in total, and not separately insured as a POD account.

The FDIC's new rules will go into effect July 1, 1998. For more information about the insurance rules in general or the changes in particular, you may contact the FDIC's Division of Compliance and Consumer Affairs listed on Page 15 of this newsletter. 

### New \$20 Bill Due in Autumn

First the \$100 and \$50 bills were redesigned, primarily to help deter counterfeiting. Now it's time for the \$20 bill to get a facelift with anti-fraud features and other improvements. The new version is scheduled to enter circulation this fall, the U.S. Treasury Department announced in April. The \$20 note is commonly used in American commerce and it's the bill most often dispensed by automated teller machines (ATMs).

The redesigned \$20, like the new \$50 bill, will include a large dark numeral on a light background on the back of the note. This will make the bill easier to identify by people with poor vision. The Treasury said that the remaining denominations — the \$10, \$5 and \$1 — also will include this low-vision feature, as will the future redesign of the \$100 note.



# New IRAs, New Insurance Determinations

## Here's how two new savings accounts will be protected by the FDIC

In our last issue, we noted that the FDIC was looking at how the insurance rules would apply to two new types of individual retirement accounts (IRAs) that consumers can use to save for retirement or college tuition costs. We now can report our lawyers' opinions on the coverage of these two accounts.

### Roth IRAs

One way the Roth IRA differs from a traditional IRA is that contributions to a Roth IRA are not deductible from taxable income. On the other hand, for many people the earnings on a Roth IRA are tax-free whereas earnings on a traditional IRA are only tax-deferred.

While the Roth IRA has different characteristics than the traditional IRA, the FDIC Legal Division says that both will be treated the same for deposit insurance purposes. This means that the deposits you have in Roth IRAs and traditional IRAs at the same FDIC-insured bank or thrift will be added together and insured (along with certain other retirement-type accounts you may have there) up to a total of \$100,000. This IRA coverage is separate from the FDIC insurance for your other types of deposits, such as individual or joint accounts.

### Education IRAs

Think of Education IRAs as trust accounts established exclusively to pay for a beneficiary's tuition for college, graduate school or post-secondary vocational school. Generally, earnings on an Education

IRA are exempt from federal taxes if they don't exceed the student's education expenses.

For FDIC insurance purposes, an Education IRA will not be treated as a retirement-type account. Instead, it will be insured as an "irrevocable trust account" — a type of account a depositor sets up on behalf of a beneficiary and that cannot later be changed or nullified.


So, any Education IRAs and irrevocable trust accounts you have at an insured institution generally will be added together and protected for up to \$100,000 per beneficiary. This coverage is separate from the FDIC insurance given to other types of deposits (individual accounts, joint accounts, retirement accounts, etc.) that either the depositor or the beneficiary might have at that institution.

### Final Thoughts

The bottom line: If you're considering opening or adding to one of these new accounts, and you or your family have \$100,000 or more on deposit at that institution, we urge you to double-check to make sure that the funds are fully protected in the event that the institution fails.

"These types of accounts can be complex and don't always fit neatly into any of the categories of deposit insurance coverage," says Joe DiNuzzo, an FDIC attorney in Washington and an expert in the deposit insurance rules. "Depositors with more than \$100,000 at one

insured bank or thrift should familiarize themselves with the deposit insurance implications involved."

For more information about these types of accounts, including the pros, cons, qualifications or tax implications, we suggest that you consult with your accountant, attorney, financial planner or other advisor. For more information about deposit insurance on these or any other accounts, you can contact the FDIC's insurance experts in the Division of Compliance and Consumer Affairs (see Page 15). 

### Financing College... A Test With Multiple Choices

Please send us your suggestions for easing the burden of paying for higher education. Also, feel free to share any money-management tips for parents and their fledgling financiers on their first flight out of the nest. Or, let us know if you have questions you'd like answered in our upcoming feature.

Write by July 15th to:  
Jay Rosenstein, Editor  
FDIC, 550 17th Street, NW,  
Washington, DC 20429  
Internet: [jrosenstein@fdic.gov](mailto:jrosenstein@fdic.gov)  
Fax: (202) 898-3870

Please include your name, address, and phone number. No names will appear in print without permission.



# ATM Fees Don't Have to be Automatic


## Here are a few ways to minimize charges at the teller machine

**S**tudies indicate that ATM “access fees” or “surcharges” are becoming more common and more expensive for consumers who use teller machines that aren’t owned by their bank. The fees typically run \$1.50 per transaction — although you can pay upwards of \$3 or more — and they’re automatically deducted from your account. Banking institutions mostly charge these fees to non-customers to offset the costs of owning and running the machines. These fees can add up, especially for frequent users of ATMs. What can you do to minimize ATM fees?

- Use your own institution’s ATMs whenever possible. Nearly all banks offer unlimited free transactions for their own customers.
- If you use ATMs owned by institutions other than your own, try to use those that don’t charge a fee to

non-customers. How will you know which ones won’t charge a fee? You should see a sign at the ATM disclosing whether surcharges are imposed on non-customers, and you’ll have the opportunity to “opt out” of a transaction at no charge. If you have time to do some research before going to the ATM, call your bank and ask for names of other institutions that won’t charge you a fee. Or, you can look on the Internet for lists of surcharge-free ATMs. Two such Internet services we know of are from Bank Rate Monitor ([www.bankrate.com](http://www.bankrate.com)) and Sundin Associates ([www.surcharge-free-atms.com](http://www.surcharge-free-atms.com)).

- Consider withdrawing larger sums each time (\$100 or \$200 instead of \$20 or \$40) so you’ll make fewer trips to the ATM and save on the transaction fees.

- If your bank is one of the few that charges its own customers for ATM use, try to conduct your business inside with a human teller whenever possible. Remember, though, that a few banks charge a teller fee, too.
- Consider paying for purchases with personal checks, traveler’s checks, debit cards (which deduct automatically from your account) and credit cards. Many grocery stores now also let you get cash back when you pay by check or debit card. Remember, though, that these other options may carry their own fees, such as interest charges on credit card balances if you don’t pay at the end of the month.
- If you plan to use machines a lot, find out if your bank or other institutions offer special accounts or features for ATM users. Fees can vary, so shop around. 


## FDIC Enhances Access to Community Reinvestment Reports on the Internet

The FDIC has a new Internet service giving the public quick and easy access to Community Reinvestment Act (CRA) evaluations for the approximately 6,000 banks supervised by the agency. The CRA requires federal regulators to assess and rate an institution’s record of helping to meet the credit needs of its entire community, including low- and moderate-income neighborhoods, consistent with safe and sound lending. The regulators also are required to make public each institution’s CRA rating and the detailed performance evaluation that led to the rating.

With the new Internet service, you can quickly obtain the latest rating for a single bank or a group of banks by keying in certain information. You can, for example, search for the CRA ratings of all the FDIC-supervised banks headquartered in your city or state. You also can obtain CRA performance evaluations dating back to 1996.

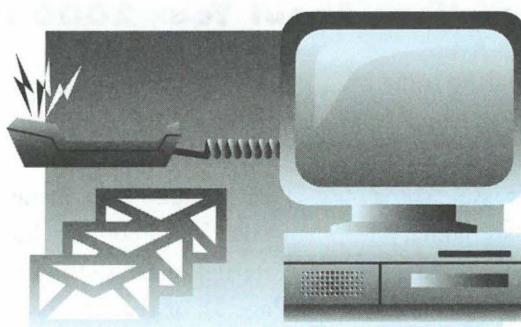
To get the FDIC’s CRA ratings and evaluations on the Internet, go to [www.fdic.gov/publish](http://www.fdic.gov/publish), then click on “Community Reinvestment Act” followed by “Automated CRA Ratings Search.” Questions may be e-mailed to [consumer@fdic.gov](mailto:consumer@fdic.gov) or

directed to the FDIC’s Division of Compliance and Consumer Affairs at (800) 934-3342. To get to the other agencies’ evaluations on the Internet, go to [www.ffiec.gov/cra/info](http://www.ffiec.gov/cra/info).

If you don’t have access to the Internet, you can get a copy of an institution’s CRA evaluation directly from that institution or its primary federal regulator. You may be charged a nominal fee. For a copy of CRA information from the FDIC, please mail or fax a request to our Public Information Center listed on Page 3. Names and addresses for other federal regulators appear on the right. 



**For questions about consumer or civil rights laws, or complaints involving a specific institution:** First attempt to resolve the matter with the institution. If you still need assistance, write to the institution's primary regulator listed on this page. Although the FDIC insures nearly all banks and savings associations in the United States, the FDIC may not be the primary regulator of a particular institution. The regulators enforce consumer protection and civil rights laws, including prohibitions against discriminatory lending practices; initiatives to prevent unfair or deceptive



practices in deposit-taking or lending; and rules that encourage institutions to meet local credit needs.

**For questions about deposit insurance coverage:** The FDIC offers protection to consumers by insuring deposits up to \$100,000 at federally insured banks and savings associations. For more information, contact the FDIC's Division of Compliance and Consumer Affairs listed below. The National Credit Union Administration insures deposits up to \$100,000 at federally insured credit unions and can be contacted at the address below.

## Federal Deposit Insurance Corporation

### Federal Deposit Insurance Corporation

Supervises state-chartered banks that are not members of the Federal Reserve System. Insures deposits at banks and savings associations.

**FDIC**  
550 17th Street, NW  
Washington, DC 20429

**Home Page:** [www.fdic.gov](http://www.fdic.gov)

**For information about consumer protections, including deposit insurance:**

**FDIC Division of Compliance and Consumer Affairs**  
550 17th Street, NW  
Washington, DC 20429

**Phone:** (800) 934-3342 or  
(202) 942-3100

**Fax:** (202) 942-3427 or  
(202) 942-3098

**E-mail:** [consumer@fdic.gov](mailto:consumer@fdic.gov)

**For questions, concerns or complaints about the Federal Deposit Insurance Corporation:**

**FDIC Office of the Ombudsman**  
550 17th Street, NW  
Washington, DC 20429

**Phone:** (800) 250-9286 or  
(202) 942-3500

**Fax:** (202) 942-3040 or  
(202) 942-3041

**E-mail:** [ombudsman@fdic.gov](mailto:ombudsman@fdic.gov)

## Other Key Regulators

### Office of the Comptroller of the Currency

Charters and supervises national banks. (The word "National" appears in the name of a national bank, or the initials "N. A." follow its name.)

**Customer Assistance Unit**  
1301 McKinney St., #3710  
Houston, TX 77010

**Phone:** (800) 613-6743  
**Fax:** (713) 336-4301

**Home Page:**  
[www.occ.treas.gov](http://www.occ.treas.gov)

**E-mail:**  
[consumer.assistance@occ.treas.gov](mailto:consumer.assistance@occ.treas.gov)

### Federal Reserve System

Supervises state-chartered banks that are members of the Federal Reserve System.

**Division of Consumer and Community Affairs**  
20th St. and  
Constitution Avenue, NW  
Washington, DC 20551

**Phone:** (202) 452-3693  
**Fax:** (202) 728-5850

**Home Page:**  
[www.bog.frb.fed.us](http://www.bog.frb.fed.us)

### National Credit Union Administration

Charters and supervises federal credit unions. Insures deposits at federal credit unions and many state credit unions.

**Office of Public and Congressional Affairs**  
1775 Duke Street  
Alexandria, VA 22314

**Phone:** (703) 518-6330  
**Fax:** (703) 518-6409

**Home Page:** [www.ncua.gov](http://www.ncua.gov)

**E-mail:** [pacamail@ncua.gov](mailto:pacamail@ncua.gov)

### Office of Thrift Supervision

Supervises federally and state-chartered savings associations plus federally chartered savings banks. (The names generally identify them as savings and loan associations, savings associations or savings banks. Federally chartered savings associations have the word "Federal" or the initials "FSB" or "FA" in their names.)

**Consumer Affairs Office**  
1700 G Street, NW  
Washington, DC 20552

**Phone:** (800) 842-6929 or  
(202) 906-6237

**Home Page:**  
[www.access.gpo.gov/ots](http://www.access.gpo.gov/ots)


**E-mail:** [consumer.complaint@ots.treas.gov](mailto:consumer.complaint@ots.treas.gov)

Some banking matters may involve state laws. For assistance, contact the appropriate state financial institution regulatory agency or state Attorney General listed in your telephone book and other directories.



## FDIC Brochure to Answer Questions About Year 2000 Date Change

The FDIC soon will publish a brochure answering some of the questions bank customers may have about the Year 2000 (or Y2K) date change and its impact on businesses like banks and savings institutions. (As noted in our last issue, some computer systems may incorrectly read the date January 1, 2000, as January 1, 1900. That may cause malfunctions in services provided by businesses, utilities and other organizations.) The FDIC brochure explains the steps that financial institutions and federal regulators are taking to

assure that computer systems will work properly come January 1, 2000. It also includes a reminder that the FDIC insures deposits up to \$100,000 against loss due to the failure of an insured bank or savings association. For your free copy of our Year 2000 brochure, please send a request by mail, Internet or fax to the FDIC's Public Information Center (see Page 3), or read the brochure on the FDIC's Internet site ([www.fdic.gov](http://www.fdic.gov)). The brochure is expected to be available in late July of 1998. 

**FDIC** *consumer news*

**BULK RATE**  
**MAIL**  
Postage & Fees  
Paid Permit  
No. G-36

**FDIC**  
Federal Deposit Insurance Corporation  
Washington, DC 20429-9990  
OFFICIAL BUSINESS  
Penalty for Private Use, \$300