



Consumer News

FDIC LIBRARY

Summer 2000

JUN 2 ~ 2000

WASHINGTON D.C.

When a Criminal's Cover Is Your Identity

ID theft puts an ugly face on your good name. A con artist who knows your Social Security number, bank account information or other personal details *can temporarily become you* in order to commit fraud. Fixing the damage could take years. Here's how to reduce your risk.

Your good name and reputation are among your most valuable assets. Unfortunately, criminals know the value of a good name and reputation, too. That's why increasing numbers of con artists are "stealing" identities. These robbers typically start by using theft or deception to learn a person's Social Security number, date of birth or other personal information. Armed with those details, the perpetrators can open credit card accounts, make

purchases, take out loans, or make counterfeit checks and ATM cards in *your* name. In effect, the crook *becomes you* in order to commit fraud or theft.

Federal and state laws plus banking industry practices may limit your losses from ID theft. For example, under the Truth in Lending Act, if a crook opened a credit card account in your name and ran up thousands of dollars in charges, the most you'd owe is \$50—and many creditors will agree to excuse you of all liability. Still, innocent victims are likely to face long hours (and sometimes years) closing tarnished accounts and opening new ones, fixing credit records, and otherwise cleaning up the damage. They also may find themselves being denied loans, jobs and other opportunities because an identity theft ruined their reputation and credit rating.

Consider these examples cited by the Federal Trade Commission

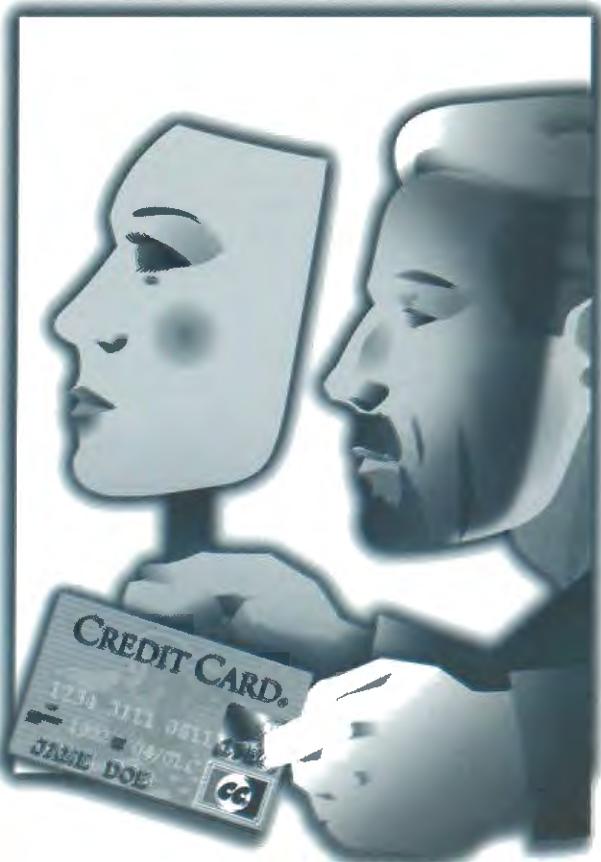


Illustration: T.W. Ballard

INSIDE

New rules to help protect your financial privacy
PAGE 6

Test your financial savvy with our latest quiz
PAGE 7

Fewer credit cards offer a "full" grace period
PAGE 10

Conditions in "living trusts" can limit insurance coverage
PAGE 10

(FTC) in congressional testimony:

- A NASA engineer was refused a loan by his bank of 11 years and had to use his retirement funds to finance his son's education.
- A consumer spent three years trying to repair her damaged credit rating and was deprived of the chance to buy what she described as her dream home.

continued on next page

• A department store clerk whose identity had been assumed by a shoplifter spent years unsuccessfully seeking employment in the retail industry.

"The problem with identity theft is that it can happen to you before you know it, and it can take a long time to correct," adds John Kotsiras, an FDIC consumer affairs specialist in Washington.

FDIC Consumer News has warned readers about identity theft before. We are highlighting ID theft again because the problem appears to be getting more common—largely because the Internet and other forms of electronic commerce have made it easier for sophisticated crooks to access Social Security numbers and other personal information. "Like any other crime or risk, identity theft is not totally preventable," says FDIC Washington-based fraud investigator Vincent Filippini. "But, there are some things a consumer can do to help prevent ID theft or make it difficult to happen."

A Checklist for Prevention

Here are seven things you can do to minimize your risk of becoming a victim of ID theft:

1 Protect your Social Security number, credit card numbers, account passwords and other personal information.

Never divulge this kind of information unless you initiate the contact with a person or company you know and trust. A con artist can use these details and a few more, such as your mother's maiden name, to withdraw money from your bank account or order new credit cards or new checks in your name.

Use common sense, and be suspicious when things don't seem right. If you get an unsolicited offer that sounds too good to be true and asks for bank account

numbers and other personal information before you receive anything in return, this is likely to be a scam. Likewise, if a caller claims to represent your financial institution, the police department or some similar organization and asks you to "verify" (reveal) confidential information, hang up fast and consider reporting the incident (see the next page). Real bankers and government investigators don't make these kinds of calls. Example: Your credit card company is unlikely to call *you* to ask for your credit card number because it already has that information.

Social Security numbers (SSNs) are especially hot items for identity thieves because they often are the key to getting new credit cards, applying for federal benefit payments, or opening other doors to money. The Social Security Administration says that consumer complaints about the alleged misuse of SSNs are rising dramatically, from about 8,000 in 1997 to more than 30,000 in 1999.

So, be very careful with your Social security number. Your employer will probably need it to report your income to the IRS, while your bank or stockbroker

may need it to report dividends or interest income. But, beyond that, such as when a business asks for your SSN in connection with a purchase, the decision is up to you... and it's a decision you should not take lightly.

"Giving your number is voluntary, even when you are asked for the number directly," says the Social Security Administration. "If requested, you should ask why your number is needed, how your number will be used, what law requires you to give your number and what the consequences are if you refuse."

Perhaps the worst that can happen if you say "no" to a merchant or service provider that wants to see your SSN is that you'll have to take your business elsewhere. Also be aware that some states that use Social Security numbers on their driver's licenses now also allow people to apply for a different number. "Getting an alternate number adds some protection from prying eyes, particularly because many merchants want to record driver's license information when accepting checks," says Gene Seitz, an FDIC fraud investigator in Washington.

Real People, Real Problems from ID Theft

These complaints were sent to the Federal Trade Commission:

"Someone used my Social Security number to get credit in my name... I have been turned down for jobs, credit, and refinancing offers. This is stressful and embarrassing. I want to open my own business, but it may be impossible with this unresolved problem hanging over my head."

"My elderly parents are victims of credit fraud. We don't know what to do. Someone applied for credit cards in their name and charged nearly \$20,000. Two of the card companies have cleared my parents' name, but the third has turned the account over to a collection agency. The agency doesn't believe Mom and Dad didn't authorize the account. What can we do to stop the debt collector?"

"Someone is using my name and Social Security number to open credit card accounts. All the accounts are in collections. I had no idea this was happening until I applied for a mortgage. Because these 'bad' accounts showed up on my credit report, I didn't get the mortgage."

2 Minimize the damage in case your wallet gets lost or stolen.

Don't carry around more checks, credit cards or other bank items than you really expect to need. Limit the number of credit cards you carry by canceling the ones you don't use. Don't carry your Social Security number in your wallet or have it pre-printed on your checks. Pick passwords and "PINs" (Personal Identification Numbers) that will be tough for someone else to figure out—don't use your birth date or home address, for example. Don't keep this information on or near your checkbook, ATM card or debit

card. Also, don't leave your wallet unattended in a store, restaurant, office or other public place—not even for a few minutes.

3 Protect your incoming and outgoing mail.

Those envelopes may contain checks, credit card applications and any number of other items that can be very valuable to a fraud artist. How can you keep mail out of the wrong hands? Among the simplest solutions: Promptly remove mail from your mailbox after it has been delivered. If you're going to be away on vacation or some other travel, have your mail held at your

continued on next page

Who to Call to Report a Possible ID Theft

If you think you're a victim of identity theft or if you notice something suspicious, get to a phone and call the following:

- **The Federal Trade Commission.** The FTC is the federal agency responsible for receiving and processing complaints by people who believe they may be victims of identity theft. Trained counselors will provide information on the steps you should take to resolve problems and repair damage to your credit record. Certain cases may be referred to law enforcement agencies, regulatory agencies or private entities that can help. Call toll-free 877-IDTHEFT (438-4338). The FTC also maintains the U.S. government's central Web site for information about identity theft at www.consumer.gov/idtheft. Go there to fill out an online consumer complaint form or link to educational materials.
- **The three major credit bureaus.** Ask them to place a fraud alert in your file, so that lenders and other users of credit reports will be careful before starting or changing accounts in your name. The special toll-free numbers for the fraud departments are: Equifax at (800) 525-6285, Experian at (888) 397-3742 and Trans Union at (800) 680-7289.
- **Your bank, credit card company or any other financial institution that may need to know.** Ask to speak with someone in the security or fraud department, and follow up with a letter. If necessary, close old accounts and open new ones, and select new passwords and "PIN" numbers (Personal Identification Numbers). Your call also alerts the financial institution to a possible scam that may be targeting other customers.
- **Your local police or the police where the identity theft occurred.** Fill out a police report that will detail what happened. Get a copy of the completed report because that can help you clear up questions and problems when dealing with your creditors and other financial institutions.

FDIC

Consumer News

Published by the Federal Deposit Insurance Corporation

Donna Tanoue, Chairman

Phil Battey, Director,
Office of Public Affairs (OPA)

Elizabeth Ford, Assistant Director, OPA

Jay Rosenstein, Writer-Editor

Tommy Ballard, Graphic Design & Illustration

FDIC Consumer News is produced by the FDIC Office of Public Affairs 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**.

Send comments, suggestions or questions to: Jay Rosenstein, FDIC, 550 17th Street, NW, Washington, DC 20429
E-mail: jrosenstein@fdic.gov
Fax: (202) 898-3870

Subscriptions

Subscriptions are available free of charge. Send subscription requests or address changes to: FDIC Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434
Phone: (800) 276-6003 or (202) 416-6940
E-mail: publicinfo@fdic.gov
Fax: (202) 416-2076

On the Internet

Consumer information from the FDIC is available at www.fdic.gov. Find current and past issues of **FDIC Consumer News** at www.fdic.gov/consumers/consumer/news/index.html. To receive e-mail notification of new issues, with links to stories, write to listserve@peach.ease.isoft.com and type "Subscribe FDIC-consumernews" (include the hyphen) and your name in the message area.

local post office or ask someone you know and trust to collect your mail. Deposit outgoing mail, especially something containing personal financial information or checks, in the Postal Service's blue collection boxes, hand it to a mail carrier or take it to a local post office instead of leaving it in your doorway or home mailbox.

4 Keep thieves from turning your trash into their cash.

Thieves known as "dumpster divers" pick through garbage looking for credit card applications and receipts, canceled checks, bank statements, expired charge cards and other documents or information they can use to counterfeit or order new checks or credit cards.

So, before putting these items in the garbage bin, tear them up as best you can. "I recommend that people buy and use a shredder," says the FDIC's Filippini. "Any paper you don't need to keep that contains private information should be shredded."

5 Practice home security.

Safely store extra checks and credit cards, documents that list your Social Security number, and similar valuable items. Be extra careful if you have housemates or if you let workers into your home. Don't advertise to burglars that you're away from home. Put lights on timers, temporarily stop delivery of your newspaper, and ask a neighbor to pick up any items that may arrive unexpectedly at your home.

6 Pay attention to your bank account statements and credit card bills.

Contact your financial institution immediately if there's a discrepancy in your records or if you notice something suspicious, such as a missing payment or an unauthorized withdrawal. While federal and state laws may limit

How to Avoid ID Theft on the Internet

The Internet offers consumers convenient ways to shop, bank and communicate. But, it also offers con artists new opportunities to quickly and secretly obtain Social Security or credit card numbers, account passwords and other personal information that can be used for fraudulent purposes. How can you protect yourself from ID theft online?

- Be suspicious of offers on Web sites or in e-mails that seem too good to be true, such as exceptionally high interest rates for deposits or ridiculously low interest rates on credit cards. They're likely to be scams attempting to get your existing account numbers or other personal information.
- Before responding to an Internet offer, determine if the business is a legitimate company or financial institution. "When you go into a store or office it's fairly easy to know if you're dealing with a legitimate company, but on the Internet it's much more difficult to determine who you're dealing with," says Cynthia Bonnette, a bank technology specialist with the FDIC in Washington. If you don't have personal references for the site, contact a federal or state consumer protection agency or your local Better Business Bureau (BBB). To be sure a Web site belongs to a legitimate company—and not to con artists—consider calling the company using a number from the phone book, a government agency or some other trusted source, not the one provided on the Web site (in case the site is a scam). Many Web sites also display seals showing they've been certified for reliability or privacy by an independent organization, such as the BBB (www.bbbonline.org), the American Institute of Certified Public Accountants (www.cpawebtrust.org) or TRUSTe (www.truste.org), a group dedicated to addressing consumer concerns about online privacy.
- Only use your credit card number, Social Security number or other sensitive information online when it's absolutely necessary. Also read the Web site's privacy policy to be sure the information you send is being "encrypted" (scrambled) so it can't be read by outsiders.
- Check the Web site's privacy policy for details about how your personal information would be protected after it's received. "Sensitive information must be stored securely and only people with a need to know should have access to the information stored in the company's files and computer systems," says Bonnette. She notes that companies must adhere to their published privacy policies or they may face penalties for unfair and deceptive business practices.
- Keep your passwords and "PINs" (Personal Identification Numbers) confidential and secure. Avoid passwords and PINs that will be easy for a thief to figure out. For example, don't use your name, street address or birth date. Also change your passwords periodically.
- Report suspected Internet-based fraud to the Federal Trade Commission (see the box on Page 3) or to the Internet Fraud Complaint Center (www.ifccfbi.gov/Default.asp), a new joint project of the FBI and the National White Collar Crime Center.

your losses if you're victimized by a bank fraud or theft, sometimes your protections are stronger if you report the problem quickly and in writing.

Also, contact your institution if a bank statement or credit card bill doesn't arrive on time because that could be a sign someone has stolen account information and changed your mailing address in order to run up big bills in your name from another location.

7 Review your credit report approximately once a year.

Your credit report (prepared by a credit bureau) will include identifying information (such as your name, address, Social Security Number, and date of birth) as well as details about credit cards and loans in your name and how bills are being paid. You should make sure the report is accurate, and that includes monitoring it for unauthorized bank accounts, credit cards and purchases.

Also look for anything suspicious in the section of your credit report that lists who has received a copy of your credit history. There are at least two reasons why:

First, identity thieves sometimes will fraudulently obtain credit reports—and valuable details that can be used in a financial scam—by posing as a landlord, employer or someone else who has a legal right to the information.

"Remember, we're dealing with people who are masters of the con game and who see consumer protection rules as simply obstacles to overcome," notes the FDIC's Filippini.

Second, crooks sometimes apply for loans or apartments in someone else's name as a way to test that person's vulnerability. "An inquiry to a credit bureau about a loan or a lease you didn't apply for could be a sign that a thief is 'casing' your credit history

to see if you have the right background to be a potential target," Filippini explains.

To order your report, call the three major credit bureaus at these toll-free numbers: Equifax at (800) 685-1111, Experian at (888) 397-3742, or Trans Union at (800) 888-4213. By law, the most you can be charged for a copy of your report is \$8.50. To be safe, consider getting a copy from each of the three companies. If after reviewing your report you

spot signs of a possible fraud, contact the organizations listed on Page 3.

Final Thoughts

Cases of stolen identity don't occur just in the movies or mystery novels. They happen to real people, and ever more frequently. We've tried to give you some of the best, easiest ways to protect your good name. Don't let ID theft take on a life of its own—yours. ■

For More Information about Stopping ID Theft

These are among the federal and state government agencies that have publications, Web sites, staff and other resources that help answer your questions on ID theft and other financial fraud:

- **Federal Regulators of Depository Institutions.** To get assistance from the FDIC, Federal Reserve Board, Office of the Comptroller of the Currency, Office of Thrift Supervision or the National Credit Union Administration, see the listings on Page 11. Past issues of *FDIC Consumer News* also have stories on some of the best ways to protect yourself from a variety of financial scams and thefts. Check them out at www.fdic.gov/consumers/consumer/news/index.html on the FDIC's Web site.
- **The Federal Trade Commission.** The FTC is a central U.S. clearinghouse for information on preventing and reporting identity theft, with a new Web site at www.consumer.gov/idtheft and a specially staffed toll-free hotline at 877-IDTHEFT (438-4338). The FTC also has several excellent publications about avoiding frauds, but start with the new booklet "ID Theft: When Bad Things Happen to Your Good Name." It's available online from the Web site, by calling the ID theft hotline, or by writing the FTC's Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. The FTC Web site also provides links to the Internet offerings of other government and private organizations that help combat identity theft.
- **The U.S. Department of Justice and the FBI.** The Justice Department, which prosecutes federal fraud cases, and its Federal Bureau of Investigation, which investigates suspected ID thefts, have posted useful information on the Internet at www.usdoj.gov/criminal/fraud/idtheft.html. To speak with someone at a local field office of the FBI, check the government listings in your local telephone book.
- **The Social Security Administration.** Under certain circumstances, the SSA will assign new Social Security numbers to victims of ID theft. To get more information about Social Security numbers and identity theft, call the SSA's toll-free fraud hotline-800-269-0271 or visit its www.ssa.gov Web site.

New Rules to Help Protect Your Financial Privacy

The FDIC and other federal regulators have issued new rules to inform consumers about their rights to financial privacy, including when and how they can prevent an institution from sharing personal information with other companies.

The rules will implement privacy-related sections of the Gramm-Leach-Bliley Act of 1999. With that law and the new rules, the federal government is trying to strike a balance between the individual's desire for privacy and the benefits to consumers in general from the free flow of information. "Many in the financial industry argue that the unrestricted flow of data results in cost efficiencies, convenience, competition and innovation in financial services," says Deanna Caldwell of the FDIC's Division of Compliance and Consumer Affairs. "The new privacy rules give individuals a voice and a choice in this debate for the first time."

The new law requires financial institutions to explain their privacy policies to customers when accounts are opened and at least once a year thereafter. These written notices must clearly describe the financial institution's practices and policies about collecting and sharing "nonpublic personal information." For example, a typical disclosure might explain that your bank shares information about your account balance, payment history and credit card purchases with non-financial companies, such as retailers, direct marketers and publishers.

Of special importance is a provision of the law that gives consumers the right to block an

institution's disclosure of private information to companies not affiliated with that institution. This process is known as "opting out." Under the new rules, even people who are not technically customers of a financial institution—such as former customers or people who applied for but didn't obtain a loan or credit card—will have the right to opt out of information sharing with outside companies. This authority to opt out does not apply to all information sharing with outside firms. For example, the law allows the sharing of information with nonaffiliated third parties to market the institution's products, handle its data processing or mail account statements.

While the rule becomes effective November 13, 2000, compliance

will be voluntary until July 1, 2001, primarily to give institutions extra time to prepare for the new privacy standards.

The rules were issued jointly by the FDIC, the Office of the Comptroller of the Currency, the Federal Reserve Board and the Office of Thrift Supervision. The National Credit Union Administration, the Federal Trade Commission and the Securities and Exchange Commission will have comparable rules for the institutions and companies they regulate that provide financial products or services. Under the FTC's rule, for example, credit bureaus are limited in their ability to sell nonpublic personal information to third parties such as direct mail and telemarketing companies. ■

New on the Net

These new federal Web sites can help you manage your money:

- As part of the FDIC's ongoing efforts to help the public with banking-related questions or concerns, we've developed a new Customer Assistance page at www.fdic.gov/consumers/questions/customer/index.html. You'll find links to information that can provide immediate answers to questions. For more assistance, send questions using the same page's Customer Assistance Form.
- When planning for retirement, it helps to know in advance how much money you can expect to receive each month in Social Security benefits. Check out the U.S. Social Security Administration's "Retirement Planner" site at www.ssa.gov/retire and use one of its online calculators to estimate your future Social Security benefits under different scenarios, such as how many more years you're likely to work.
- The Treasury Department's Web page at www.savingsbonds.gov offers new services that make it easier to buy U.S. Savings Bonds and manage your portfolio. Click on the "Savings Bond Connection" to purchase bonds any time, using your Visa or MasterCard. If you want to buy a bond as a gift but you can't wait a week for it to arrive in the mail, you can download a Savings Bond gift certificate. (Remember, you can also buy Savings Bonds and gift certificates the traditional way at banks and other financial institutions.) The Treasury's Web site also has a "Savings Bond Calculator" that will list your bonds, automatically update their values and let you know when a bond has stopped earning interest.



Test Your Financial Savvy

Think you're pretty sharp when it comes to bank products, deposit insurance, your rights as a consumer, and ways to avoid financial fraud? Find out how well prepared you really are.

1 Which two of the following products and services offered by banks are eligible for FDIC insurance?

- A. Safe deposit boxes.
- B. Mutual funds and annuities purchased from an FDIC-insured institution.
- C. Mutual funds that invest only in U.S. government securities.
- D. A certificate of deposit issued by an insured bank but obtained from a brokerage firm.
- E. A money market deposit account.

2 The basic FDIC insurance limit is \$100,000 for...

- A. Each account you have at an insured institution.
- B. Each ownership category of account you have at one insured institution. That means you'd get \$100,000 of coverage for your individual accounts, \$100,000 for your part of any joint accounts, and so on.
- C. All your money at all FDIC-insured institutions combined.

3 You get a letter saying you've been "pre-approved" for a card with a very high credit limit and a very low Annual Percentage Rate (interest rate). What does it mean if you've been pre-approved?

- A. You're guaranteed to get that credit card at the credit limit and interest rate featured in the letter. All you need to do is call or write the card issuer and say "sign me up."

B. You're definitely guaranteed to get a credit card but, upon further review of your finances, the card issuer can instead offer you a card with less-attractive rates and terms.

C. You're not guaranteed a card. You first must send in an application and undergo a credit check. If your application is approved, you can be offered a card with less-attractive rates and terms.

4 Federal laws restrict the amount of interest and service charges that credit card issuers can charge consumers. True or false?

- True
- False

5 When you apply for a credit card, auto loan, mortgage or any other type of loan, the lender probably will look at your "credit report" from a credit bureau that describes your financial reliability, such as how timely you are with bill payments. How often do most experts say you should get a copy of your credit report to be sure it's accurate?

- A. Every time you apply for a loan—no matter how frequently (or infrequently) that is.
- B. Approximately once a year.
- C. Only about once every five years, because the basic information in the report doesn't change much from year to year.

6 You find proof of a bank account that a deceased relative had 20 years ago. You're not sure if this account

was closed or if it's forgotten money that can still be claimed. Which of the following is true?

A. The bank is required to keep savings accounts indefinitely. So, if the account wasn't closed by your relative, the money will be there waiting to be claimed.

B. Under the typical state law, if a bank account is "inactive" for about five years, and efforts to reach the owner are unsuccessful, the bank will transfer the funds to a state unclaimed property office.

C. Under the typical state law, the bank must keep an inactive account open for at least 20 years before transferring the funds to the state.

7 You're surfing the Web and you come across a site for an unfamiliar bank that offers attractive deals on a deposit account or a credit card. Before you send money or file a credit card application, how can you be sure the bank and the Web site are legitimate?

A. E-mail the Web site or call the phone number listed on the site and ask if the bank is legally authorized to do business in the U.S.

B. First contact a federal or state bank regulatory agency to confirm that the bank is legitimate. If it is, next make sure the Web site belongs to that same bank by calling the institution directly, using a phone number provided by the government, the phone book, directory assistance or some other trusted source.

C. Either of the above.

Answers on next page

Answers to Our Quiz

1 D and E. FDIC insurance only applies to funds that are placed on deposit at FDIC-insured institutions. These deposits include checking accounts, savings accounts, money market deposit accounts (a transaction account limited to six transfers per month) and certificates of deposit (CDs). Under the FDIC's deposit insurance rules, it's also permissible for brokerage firms to place funds for customers in insured accounts at banking institutions, even though the brokerage firm itself is not a member of the FDIC. There are special rules governing so-called "brokered deposits," so for more information, consult the FDIC's resources listed on the next page.

Why aren't mutual funds, annuities or the contents of safe deposit boxes protected by FDIC deposit insurance? Mutual funds and annuities are types of investments—not deposits—and therefore they are not guaranteed against loss by the FDIC, even if they are sold to you in the lobby of an FDIC-insured institution. As for safe deposit boxes, think of them strictly as storage space. Even if you stored cash or checks in a safe deposit box at an insured institution, they still wouldn't qualify as deposits under the insurance laws. Among the reasons: Deposits are intended for the bank to use to make loans to other customers.

2 B. Under FDIC rules, there is \$100,000 of deposit insurance for each category of a customer's deposit accounts (including principal and accrued interest) at an institution. The most common categories are individual accounts, joint accounts, testamentary accounts (often called "payable-on-death" accounts), and retirement

accounts (including Individual Retirement Accounts, Keoghs, and pension or profit-sharing plans). So, you can have more than \$100,000 of coverage in the same institution, depending on the account types and how they're owned. Remember, too, that the funds you hold in separately chartered institutions are always separately insured from each other.

3 C. Just because you're pre-approved for a credit card doesn't mean you're guaranteed a card or the rates and terms touted in the promotion. Being pre-approved means that a "pre-screening" by the card company indicates you may meet the criteria it wants in a customer. But, as explained in the promotion, you still must apply for the card and await the results of a credit check before finding out what you're truly approved for, if anything. Many consumers don't see or hear the words in the sales pitch explaining that a pre-approved offer is a conditional offer only.

What if, after applying, the card company offers you a less-attractive card instead? "You can always call or write the company about the terms they offered you," says Janet Kincaid, a credit card specialist with the FDIC in Kansas City. "Try to renegotiate or ask what criteria you did not meet in order to receive the original offer." If you're still not happy with the outcome, she adds, "You always have the right to refuse the new terms."

4 False. The federal Truth in Lending Act requires credit card issuers to disclose their interest rates, fees and other account terms, and to give card holders advance notice, typically at least 15 days, before changing the card's features. (In the case of a variable-rate card, no advance notice is required to change the rate.) But, when it comes to *how much* the card issuer can charge,

that's only subject to your card agreement (a contract that you sign) and any restrictions on rates and fees under state law where the card issuer is chartered. That's why we advise consumers to read the documents sent by the card company and to try to understand as much as possible about the card's main features.

"Many consumers who contact the FDIC admit they didn't read the card agreement, or they complain that an employee told them one thing when the paperwork said something else," says Cora Lee Page, an FDIC consumer affairs specialist in San Francisco. "Consumers need to know that if they sign a form without reading it they are hurting themselves if a dispute later arises."

5 B. Most experts say you should get a copy of your credit report about once a year. Why? A regular review of your credit report helps reveal if a thief has been using your name for fraudulent purposes. (See our cover story about identity theft for more details.) Your credit report also is a reflection of your financial responsibility, so you want it to be complete and accurate. And, because you never know when you'll be in a rush to get your next credit card or loan, you can head off potential problems and delays by periodically looking at your report to supply missing details or fix inaccurate information.

There are three major credit bureaus that financial institutions rely on for credit reports. Call any of them toll-free for a copy of your credit report: Equifax at (800) 685-1111, Experian at (888) 397-3742, or Trans Union at (800) 888-4213. The most you can be charged for a credit report under current law is \$8.50. Credit report content may vary significantly among the credit bureaus, so you may want to request copies from all three.

6 B. "Many people incorrectly believe that a financial institution just keeps accounts open forever and the money is sitting in the bank's vault waiting for them to come and get it," says Kathleen Halpin, an FDIC insurance claims agent based in Dallas. In reality, state laws require banks to transfer inactive accounts to the state government where the depositor was last known to live. While state laws vary, this transfer would occur if there were no transactions or communications from the account owner for about five years, and the bank was unsuccessful trying to reach the owner.

How do people "lose" bank accounts in the first place? Perhaps they moved and changed names without informing the financial institution, or they were unaware the account had been set up for them as a child. But, just because you find evidence of an old account, that doesn't mean the bank or the state would have the money. Among the reasons, according to Kathleen Nagle, a consumer affairs official with the FDIC in Washington: Banks do not require depositors to turn in an original passbook or certificate to close an account. "Our experience shows that it's likely that the account was closed years ago," she says, and the depositor failed to update the records at home, leaving a lot of people wondering what happened.

When in doubt about an old account, check with the bank or the state where any unclaimed property would have been sent. If you have problems locating a particular bank, contact the FDIC's Division of Compliance and Consumer Affairs listed on Page 11. State unclaimed property offices are usually listed in your phone book (sometimes as part of the state treasurer's department). A faster alternative is an online search of many states' inventories using

www.missingmoney.com, a Web site sponsored by the National Association of Unclaimed Property Administrators.

States do attempt to reunite property owners with their assets, but even if a state eventually sells an asset (such as jewelry in a safe deposit box), the original owner or any heirs generally still have the right to claim its value from the state. There is, though, an important deadline facing people who left deposits behind in an insured bank or savings institution that failed. Under federal laws, consumers who forget about insured deposits in a failed institution and can't be located by the FDIC or the state run the risk of forfeiting the money.

How long a depositor (or an heir) has to claim the funds depends on when the institution failed. In years past, a depositor had as little as 18 months to act after an institution closed. Under new rules effective since mid-1993, however, people now have an additional 10 years—11 1/2 years in total—to claim insured funds. Forfeited money is put back into the FDIC's deposit insurance funds to pay insured depositors in future bank failures.

7 B. Some companies on the Web pretend to be banks seeking deposits but really are not legitimate institutions.

Furthermore, some thieves are using the Internet to obtain valuable personal information, such as credit card or Social Security numbers. So, before you send money or information to a bank Web site, first contact the FDIC or any federal or state banking regulator (see Page 11) to confirm that the bank named on the Web site is legitimate. One resource is our database of FDIC-insured financial institutions at www2.fdic.gov/structur/search. Also remember that there may be institutions on the Web that are not supervised by U.S. banking

regulators and are not insured by the FDIC, but they still may be legitimate, such as some foreign banks.

"But, even if you confirm that a particular bank is legitimate, that doesn't necessarily mean the Web site you have visited belongs to that bank," warns Cynthia Bonnette, a bank technology specialist with the FDIC in Washington. That's because con artists may try to confuse consumers by using company names or Web addresses that sound like familiar, legitimate organizations. So, to be sure a Web site belongs to a real bank, consider calling that bank using the number provided by a banking regulator, the phone book, directory assistance or some other trusted source. Do not use the phone number or e-mail address shown on the Web site, Bonnette says, "because that won't be helpful if you're simply put in touch with individuals who created a fraudulent site."

Time for Some Homework?

If you want more information about topics addressed here or other issues affecting bank customers, the FDIC can help. Contact the FDIC's Division of Compliance and Consumer Affairs toll-free at 800-934-3342, or by mail at 550 17th Street, NW, Washington, DC 20429. You can also get answers to questions by visiting the FDIC's Web site. Start at the home page at www.fdic.gov or go straight to our Customer Assistance page at www.fdic.gov/consumers/questions/customer/index.html, where you'll find connections to resource materials and a form you can use to send questions electronically to the FDIC.

We hope you enjoyed our quiz. We also hope you passed with flying colors and perhaps learned something that can help you achieve your financial goals. 

Did You KNOW...?

Fewer Credit Cards Offer a "Full" Grace Period

A credit card's grace period refers to the number of days before the card company starts charging you interest on new purchases. Many consumers think that with practically every card all their purchases are interest-free for at least 25 days regardless of the previous balance. "But, the fact of the matter is it's getting harder to find a credit card that offers that kind of free ride on finance charges," says Janet Kincaid, a credit card specialist with the FDIC in Kansas City.

Some cards still offer a "full" grace period. That would mean 25 days or more of interest-free purchases, even if you're paying interest on an outstanding balance from the previous month. However, with the typical credit card nowadays, if you carry over as little as a penny from the previous month's balance you can expect to be charged interest immediately on new purchases. And, if you have a card with no grace period, you *always* pay interest on new purchases from the day you make the purchase, even if you pay your bill in full.

The bottom line: Try to understand a card's rules governing the grace period as well as the interest rate and fees. You can do this by reading the literature provided by the card issuer and, if you have questions, calling what's usually a toll-free number for customer assistance. Also, think about how you plan to use a card, especially if you expect to carry a balance most months. Then try to choose and use the card that's best for you.

Conditions in "Living Trusts" Can Limit Insurance Coverage

Since the early 1990s, Americans have increasingly been turning to revocable "living trusts" as a way to leave assets to loved ones after their death. The popularity of the living trust is due to tax and inheritance benefits, and also, because unlike a traditional trust, the owner can cancel the living trust at any time. Many consumers ask the FDIC about the insurance coverage of living trust funds—and it's a good thing they do, because they often are surprised and disappointed to learn that their living trust account does not qualify for as much insurance as they thought. Here's why:

Revocable living trust accounts are a type of "payable-on-death" (POD) account. Under the FDIC's rules, POD accounts at a particular bank or savings institution are insured up to \$100,000 per "qualifying" beneficiary, specifically the account owner's spouse, children, grandchildren, siblings and parents. This means a \$300,000 account payable on death to a spouse, a parent and a sibling would be fully insured (\$100,000 for each beneficiary). However, to get this broad coverage for POD accounts, several requirements must be met, including one that says the funds must pass directly to the named beneficiaries without conditions. Why is this usually a problem for living trust depositors?

"The typical living trust imposes conditions, such as that the beneficiary must have a college degree or be married in order to receive the funds," says Washington-based FDIC attorney Joe DiNuzzo. "Any such condition is enough to disqualify a living trust account from the POD coverage of \$100,000 per

beneficiary." In fact, DiNuzzo says, it's safe to assume a living trust account won't qualify for POD coverage unless the account details prove otherwise.

Using the example described previously, a \$300,000 account that had conditions in the living trust would be considered one of the owner's individual accounts at the bank insured to just \$100,000 in total, *not* \$100,000 per beneficiary (\$300,000) as a POD account.

For more information, DiNuzzo recommends that you read the FDIC's April 1999 guidelines on the insurance coverage of living trusts and other revocable trust accounts. The guidelines appear on the Internet at www.fdic.gov/deposit/deposits/financial/letter2.html, or a copy can be obtained from the FDIC's Public Information Center listed on Page 3 of this newsletter. For additional guidance, call an FDIC deposit insurance expert toll-free at 800-934-3342 or, for TTY, at 800-925-4618. "You also may want to ask the attorney who drafted your living trust to review the trust document in light of the deposit insurance rules," DiNuzzo says.

Direct Deposit is Safer Than Checks in the Mail

This is for consumers who like to receive their pay or benefit checks in the mail instead of having the funds directly deposited into their bank accounts. According to a U.S. Treasury Department analysis of federal benefit payments during 1999, problems with paper checks (such as getting lost, misplaced or stolen out of a mailbox) occurred 26 times more often than when the money was sent electronically. Also, the Treasury says, a lost or stolen paper check can take about two weeks to replace, while an electronic transfer problem can generally be traced and corrected within a day or two. 

For More Information



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

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.

For questions about deposit insurance coverage: The FDIC insures 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. The National Credit Union Administration insures deposits up to \$100,000 at federally insured credit unions. Addresses and phone numbers are listed on this page.

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 Street
Suite 3710
Houston, TX 77010

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

Home Page: www.occ.treas.gov

E-mail: 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 Street and Constitution Ave., NW
Washington, DC 20551

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

Home Page: www.federalreserve.gov

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

E-mail: 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.ots.treas.gov

E-mail: 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.



Federal Deposit Insurance Corporation
Washington, DC 20429-9990

OFFICIAL BUSINESS
Penalty for Private Use, \$300

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