Special Report on Fraud

FDIC Consumer News

Spring 2003

# Fighting Financial Fraud: How to Shield Yourself from Swindles

## A guide to help you defend against an array of scams involving checks, credit cards, ATMs, the Internet and other bank products and services

You probably think an educated consumer is someone who comparison shops and makes smart buying decisions. But there's more to being a savvy consumer than knowing how to find a good deal—you also need to know how to avoid a bad deal, especially a fraud.

*FDIC Consumer News* frequently publishes articles about financial scams that could affect our readers. A primary example is identity theft—far and above the top consumer fraud complaint reported to federal authorities—in which a con artist "steals" a name, Social Security number and other personal information to run up thousands of dollars in fraudulent loans or credit-card purchases.

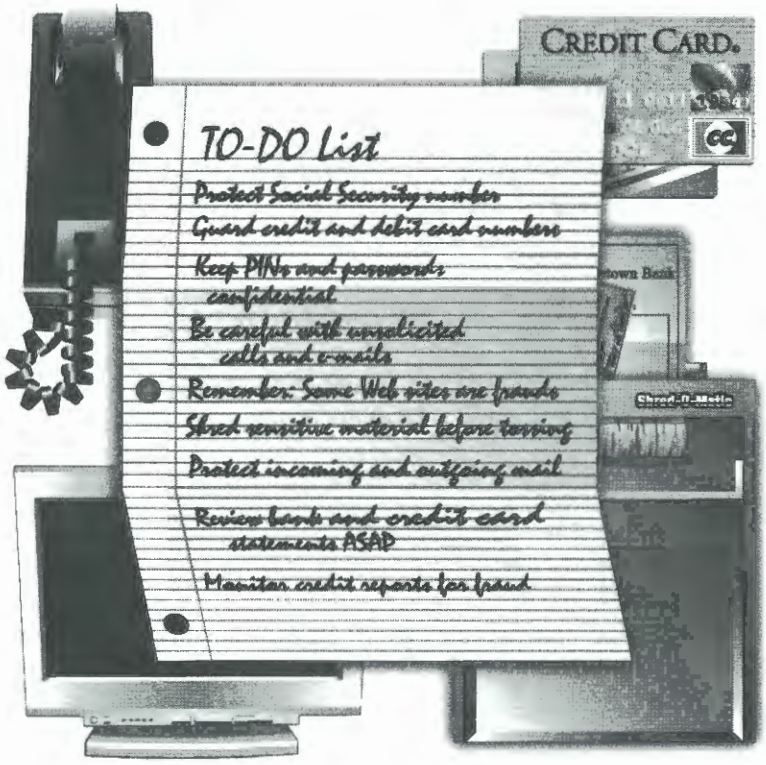


Illustration: T.W. Ballard

## INSIDE

*Common cons... and how to avoid them*
PAGE 2

*Ten simple things you can do to fight fraud*
PAGE 8

*Paying extra for ID theft protection? Consider costs vs. benefits*
PAGE 10

Given the hundreds of millions of dollars that businesses and consumers lose to swindlers each year, we are devoting this edition of our newsletter to helping you defend against an array of deceptions involving checks, credit cards, ATMs, the Internet and other bank products and services. Our goal is to enlighten, not frighten, you. We hope you'll never be the victim or even the target of financial fraud. However, to boost the odds in your favor, you should learn how to protect yourself.

We also want you to understand why you should take fraud prevention seriously. It's true that federal and state laws and industry practices limit dollar losses for crime victims in many cases. It's also true that businesses and law enforcement agencies devote tremendous resources to spotting or stopping financial fraud. And many government agencies, including the FDIC, require security procedures in the private sector to help protect

*continued on next page*

customers and their personal information. Even so:

• Not all crimes can be prevented, and some fraud victims (especially those not paying attention to their bank or credit card statements and not quickly reporting suspicious activity) will lose money;

• Fraud victims may spend a considerable amount of time (sometimes years) filling out police reports, closing old accounts, straightening out their credit records or otherwise clearing their names; and

• All consumers indirectly pay some of the cost of financial fraud in terms of higher prices for goods and services (from businesses that bear the primary responsibility for losses) and higher taxes (to pay for law enforcement).

Also remember that even if you successfully sidestepped a swindle, by taking the time to report a suspicious phone call, e-mail or other transaction you can alert the proper authorities and help keep other people from becoming victims.

Our special report features an overview of financial frauds we want consumers to know about and suggestions for how to shield yourself from most major swindles. We also have provided a review of key consumer protection laws and organizations you can contact for help or more information.

Successful con artists stay one step ahead of their victims. That's why if you are aware of the games crooks play—if you recognize the warning signs and take the proper precautions—you can protect yourself and your community from the high costs of fraud.

## Common Cons... and How to Avoid Them

*FDIC Consumer News* asked FDIC fraud investigators and other officials about common financial scams that target consumers. Here are the frauds they say should be on your watch list, plus warning signs and the best defenses for each.

### IDENTITY THEFT

***How it works:*** Identity theft is, by far, the top fraud complaint reported to the Federal Trade Commission (FTC) for the past three years. By trickery, by stealing information from mailboxes or trash, or by using publicly available information, a crook obtains personal information about you—for example, your Social Security number, date of birth and mother's maiden name. With those details, he or she may be able to obtain a copy of your birth certificate and Social Security card as well as apply for a driver's license, a passport or other form of picture ID. Or the ID thief may be able to create phony documents with your personal information. The result could be that the fraud artist is able to obtain credit cards, take out loans, make counterfeit checks or cards and go on a spending spree in your name. In effect, he or she becomes you for the sole purpose of committing fraud or theft.

This type of crime also can go undetected for many months, if not years, because bills and other documents often are sent to fake addresses, not to your house. "You may only become aware of the situation after unpaid and delinquent bills begin to accumulate and your credit record has been downgraded, and solving that problem can be a long and arduous tasks," says Kevin Hutchison, an FDIC examiner. You may even be denied a loan or credit card, an apartment, a job or other opportunities because an identity thief ruined your credit rating.

***Best defense:*** Many of the tips in this special report can help prevent ID theft. Here are examples. Protect your credit card numbers, Social Security numbers, account passwords or other personal information. Be suspicious of unsolicited offers that seem too good to be true, because they could be fraudulent attempts to get your bank account numbers or other personal information. (See Page 8 for more examples of how to protect your personal information.)

If credit cards or IDs of any kind are missing, immediately notify the issuers. Pay attention to your bank and credit card statements, and quickly report a suspected fraud. Also monitor your credit reports for signs of ID theft, such as credit cards you don't have but are listed under your name and a different address. (See Pages 9 and 10 for more about how to monitor your credit reports.)

### CHECK FRAUD

***How it works:*** A criminal steals or finds a checkbook or collects enough information about a bank account to make a counterfeit check. To pull off the fraud, the criminal also normally needs some form of identification matching the name on the checking account. You may not discover the problem until you get surprising news that your checking account is overdrawn or someone who accepted a counterfeit check with your name on it is demanding you make

good on the payment. (Also see the information on the next page about frauds involving cashier's checks and other "official" checks.)

***Best defense:*** At home, keep your supply of blank checks in a closed drawer, a safe or other secure location. Don't keep your checkbook on your kitchen counter or other open area where it can easily be seen by someone you don't know or may not trust who happens to be in your home. Around town, it's a good idea to carry only as many checks as you expect to use, and keep them in your possession at all times. Pre-print as little personal information on your checks as possible and never have your Social Security number or driver's license number pre-printed on your checks. If a stranger asks you to accept a check as payment for a significant purchase, ask for a cashier's check or similar official check instead (and take additional precautions as explained in the item about cashier's checks). Finally, it's important that you review your bank statement soon after it arrives and immediately report any unauthorized transactions. Why? "If you're not paying attention to your account and fraudulent checks keep getting through, it's possible that you, not the bank, may be held liable for the losses," warns Christy Cornell-Pape, an FDIC fraud investigator.

### ADVANCE-FEE SCAMS

***How they work***: There are many variations of this fraud but they all follow a basic script. You receive an unsolicited and extremely attractive offer of a product, service, loan, credit card, vacation, business opportunity or similar deal, but you're told you must send money (supposedly to cover fees, taxes, shipping and handling, and so on) or divulge bank account numbers before you receive anything in return. Lo and behold, the promised goods or services never arrive or they come with significant flaws.

Popular versions include fraudulent or deceptive offers of credit or credit repair to people with a poor credit history; vacation clubs that require a "membership fee" and give little or no benefit; and the so-called "Nigerian scam" involving an unsolicited e-mail or letter from someone claiming to be an official from a foreign government or corporation promising an lucrative reward (even millions of dollars) or a business opportunity if you'll "help" by paying certain up-front expenses or allowing the temporary use of your U.S. bank account (which the crooks can drain if you give them your account number).

***Best defense:*** Be extremely skeptical of any unsolicited offer that seems unrealistic and requires you to send a payment or provide bank account information before receiving a service or product. Also do NOT reply to an unsolicited letter or e-mail offering a major reward in exchange for your financial assistance or bank account information. "If an offer seems too good to be true, be careful," says Bret Morgan, an FDIC examiner. "Think about why a stranger would offer to share a fortune with you simply for the brief use of your bank account or your help paying a few thousand dollars in fees. Think about the risks involved with sending funds or sharing your account information." Morgan adds, "By using your common sense and being realistic, you will likely conclude that you'll get nothing but trouble if you participate in one of these offers."

If you get an e-mail that you believe is part of a Nigerian-type scam, you can forward a copy to

*continued on next page*

### 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, immediately get to the phone and call:

- **The police**. Get a copy of any police report or case number for later reference.
- **Your bank, credit card company or other financial institution** that may need to know. Close accounts that have been fraudulently accessed or opened.
- The fraud department at any one of **the three major credit bureaus**—Equifax at 800-525-6285, Experian at 888-397-3742 and TransUnion at 800-680-7289. The credit bureau you contact will share the information with the other two and a "fraud alert" will be placed in your credit file at all three companies so that lenders or other users of your credit records can avoid opening a fraudulent account in your name. You'll also receive a free credit report from all three companies so you can look for fraudulent entries. The three companies also pledge to work with you to delete any fraudulent information in your file.

  **Note**: If you become aware of anyone using your identity, also notify the Federal Trade Commission (call toll-free 877-ID-THEFT or 877-438-4338, or go to www.consumer.gov/idtheft). The FTC shares complaints with other law enforcement agencies.

the U.S. Secret Service, the primary U.S. government agency investigating this kind of financial fraud, at 419.fcd@usss.treas.gov. If you've already lost money to a Nigerian-type scam, call your local field office of the Secret Service, which will be listed in the blue pages of your phone book.

### CREDIT/DEBIT/ATM CARD FRAUD

***How it works***: With credit cards, a thief might use your card or obtain a new card in your name, perhaps by stealing a pre-approved card application from your mail and having the card sent to a different address. Or he or she might counterfeit your current credit card. One scenario: The crook or an accomplice might work at a retail establishment—perhaps a bar or restaurant—where the card briefly may be out of sight. This person can swipe your card through an electronic "skimming" device that captures key account information from the card's magnetic strip.

As for ATM cards (which deduct amounts taken at automated teller machines from your checking account ) and debit cards (which deduct for cash or payments transacted at ATMs or retail establishments), the perpetrator might steal an existing card or make a new one. He or she also might obtain your personal identification number (PIN)—the security code you use to authorize transactions. One way to learn your PIN is to watch over your shoulder (even with binoculars or a video camera) as you use your card. Another tactic used by criminals is to attach a keystroke recording device to an ATM or checkout register, perhaps at a gas station, convenience store or other establishment where customers may be in too much of a hurry to notice something suspicious. Yet another way to obtain a PIN is to trick a consumer into divulging the numbers in response to a deceptive call or e-mail.

***Best defense:*** Check your bank and credit card statements soon after they arrive and immediately report any unusual or unauthorized transactions. While federal law limits your liability for fraudulent credit card transactions to up to $50 per card, the rules are different for debit and ATM cards. The sooner you report an unauthorized transaction involving your debit or ATM card, the more you reduce your potential liability under the federal Electronic Fund Transfer Act (see Page 7). Remember that criminals steal credit card solicitations, bank statements and other important papers out of mailboxes, so take precautions with your incoming and outgoing mail (see Page 8). Also contact your financial institution if your credit, debit or ATM card is lost, stolen or stuck inside an ATM. Never give your credit card or debit card number or PIN in response to an unsolicited e-mail or phone call. Never write your PIN on your card or on a piece of paper in your wallet—memorize the number instead.

*The result of identity theft could be that the fraud artist is able to obtain credit cards, take out loans, make counterfeit checks or cards and go on a spending spree in your name.*

Avoid ATMs in dark or remote areas or if people seem to be loitering by the machines. Steer clear of anyone offering to "help" you carry out a transaction—it may be a setup. Also walk away if it appears that any machines may have been tampered with or if there's a sign directing you to use one of multiple machines—the one that may be rigged with a keystroke recorder or a plastic insert that grabs cards until the criminals come for them.

Be very skeptical if a retail employee swipes your credit or debit card through two devices instead of one—the second device could be a skimmer for recording your account information. If you spot a suspicious employee or machine at a retail establishment, report it to a manager or, if you still have concerns, to your card issuer's fraud department. Always take your credit, debit and ATM receipts with you—never leave them for a crook to find useful account information printed on the receipts.

### FRAUDULENT CASHIER'S CHECKS

***How they work:*** Crooks know that consumers trust cashier's checks, money orders and other official bank checks because the money is already set aside at the bank. That's why con artists are increasingly counterfeiting official checks, especially for use when dealing with consumers long-distance over the Internet but also in face-to-face transactions, such as trying to cheat someone selling a used car through an ad in the local paper. Another element of the fraud may involve a cashier's check for more than the amount due. Here's an example: You're selling a $5,000 item online to a buyer overseas who offers to pay with a cashier's check from a bank in the U.S. When the official check arrives it is for $10,000, and you are instructed to deposit the $10,000 check into your bank account and wire the excess amount to the buyer's account abroad. You comply… and later find out that the cashier's check is phony. Depending on the circumstances and state law,

*you may be held responsible for the entire amount of the fraudulent cashier's check you deposited into your account.* Using our example, you may need to reimburse the bank for $10,000, even if that's far more money than you have in your account.

***Best defense:*** Independently confirm the name, address, home number and work number of the purchaser by consulting a phone book, directory assistance, or an Internet database. Insist on an official check drawn on a local bank or a bank that has a local branch, so you can make sure it's valid. If that's not possible, call the bank where the check was purchased (get the bank's phone number from directory assistance or an Internet database, not from the person who gives you the check) and ask if the check is good. If you'd rather not call the bank, ask someone at your bank to inquire about the check.

Look for warning signs that an official check may be counterfeit. "A cashier's check for more than the amount due with a request to transfer the excess amount to another bank account is like a neon sign that says 'scam,'" according to Jeff Kopchik, a senior policy analyst with the FDIC's electronic banking branch. Other red flags: The check shows it was purchased by someone else, not the person you are dealing with. Or the check doesn't have the look or feel of a real check issued by a financial institution—perhaps words are misspelled or the paper is flimsy.

Be very cautious if you wish to wire money or hand over merchandise before the check you accepted is confirmed as paid (cleared) by your bank—a process that could take several weeks. Be especially careful if you're dealing with someone long-distance, such as over the Internet. One way to protect yourself in an Internet sale is to use a reputable online escrow service that will hold the payment until the promised goods arrive. For more information about avoiding Internet payment scams, including fraudulent escrow services, read the FTC's new "Internet Auctions" brochure (online at www.ftc.gov/bcp/conline/pubs/online/auctions.htm).

### AUTOMATED PAYMENT FRAUD

***How it works:*** Millions of consumers benefit from the overall safety and convenience of automated payment programs that authorize an electronic withdrawal from an individual's checking account to cover a recurring expense (for example, a mortgage loan or utility bill) or a one-time payment (such as merchandise purchased over the phone). Unfortunately, fraudulent telemarketers and other con artists have used the electronic payment system for their benefit, too. Here's how you could be scammed.

A crook, posing as a legitimate business or charity, establishes an arrangement with a bank to process deposits electronically. Then the criminal finds the name of your bank and your checking account numbers, perhaps by tricking you into divulging the details over the phone (in what appears to be a legitimate telemarketing sales call) or by sifting through your trash for old bank statements or checks. The con artist is now in a position to send an electronic command to your bank instructing it to debit (withdraw) a certain amount of money from your checking account and forward the funds to the perpetrator's bank account. If you're not paying attention to your bank statements, the fraud can continue until your account is drained.

***Best defense:*** Never give your checking account number to authorize an automated payment unless you initiated the contact and you know you're dealing with a reputable business or charity. Be aware that con artists try to tug at your heart—and your wallet—by contacting households about bogus fundraisers for victims of a tragic event. Shred bank statements and old checks before putting them in the trash. "You also can ask your bank to block all automated payments from your account or put a 'filter' on

*continued on next page*

## Does the FDIC Cover Losses Due to Fraud?

Consumers often ask the FDIC whether federal deposit insurance covers losses caused by fraud or robbery. By law, the FDIC only protects insured deposits if a banking institution fails. However, banks and other financial institutions typically purchase special private insurance policies to cover losses from criminal acts. Also remember that federal and state laws also may limit a consumer's losses due to fraud (see Page 7).

To learn more about what is and is not protected by FDIC insurance, read our brochure "Insured Or Not Insured," available online at www.fdic.gov/consumers/consumer/information/fdiciorn.html or obtain a copy free of charge from the FDIC's Public Information Center listed on Page 11.

automated transactions so that only those you have approved will get through," says the FDIC's Cornell-Pape.

Review your bank statement as soon as it arrives and promptly report any suspicious or unauthorized electronic transactions, says FDIC attorney Janet Norcom. That's because, under the Electronic Fund Transfer Act, if you notify your bank of an unauthorized transaction within 60 days of the date the statement containing the error is mailed by your bank, you are not liable for any loss. "But if you don't notify the institution within 60 days," Norcom says, "you may have liability for any subsequent transactions that occur after 60 days and before you notify the institution."

### INTERNET FRAUD

***How it works:*** There are numerous, inventive ways being used by Internet crooks to commit fraud. One approach involves a fraudulent Web site touting extremely attractive deals on goods, services, deposits or investments in hopes that consumers will provide a credit card number, bank account number, password or a check. Some con artists set up fake banks (on the Web or elsewhere) and use false or misleading statements to indicate they offer FDIC-insured accounts.

A variation involves a copycat Web site that deliberately uses a name or Internet address similar to, but not the same as, that of a large, well-known bank, retail store or other company. Yet another scheme uses an e-mail, which appears to be your Internet service provider or a company that you already do business with that asks you to "re-enter" your Social Security number, credit card or debit card number, or personal identification numbers (PINs). Keep in mind that some fraud artists also have been known to use the FDIC name or logo illegally to make false claims about federal insurance.

***Best defense:*** Never give money, credit card or debit card numbers, PINs or any other personal information in response to an unsolicited e-mail, no matter who it's supposedly from or how legitimate it may appear. For example, "If you already have an established relationship with a company, they should not be asking you for account numbers because they already have that information," says Michael Benardo, chief of the electronic banking branch at the FDIC.

If you're tempted by an e-mail offer that claims to be from a company you already do business with, Benardo suggests that you contact the company using a phone number or e-mail address you know is legitimate, such as one listed on a recent account statement or other literature from the company. And always be suspicious of offers that seem too good to be true—for example, an Internet deposit paying 20 percent interest when local banks and other Internet banks are paying five percent. "Common sense should tell you that no one gives you something for nothing," says the FDIC's Morgan.

Before providing your credit card or debit card number or other personal information to a Web site in a transaction you didn't initiate, double check the Web address or "URL" with another, reliable source. "Even a one letter difference in URLs could land you on a fraudulent Web site," Benardo says. Avoid a Web site that looks sloppy (such as misspelled words), doesn't include key information (a mailing address or telephone number) or has an unusually long Internet address (which could indicate it's a temporary Web site set up by a crook). Also look for information confirming that your card number will be "encrypted" (scrambled) so that it cannot be intercepted by a third party.

You can also make sure an unfamiliar company is legitimate by contacting your state's Attorney General's office or consumer affairs department (listed in your phone book) or the Better Business Bureau (www.bbb.org) where the company is located. To check out an unfamiliar banking institution, contact the FDIC (see Page 11). For more information, read the FDIC brochure "Tips for Safe Banking Over the Internet," available online at www.fdic.gov/bank/individual/online/safe.html or from the FDIC's Public Information Center (Page 11).

### PREDATORY HOME LOANS

***How they work:*** An unscrupulous lender—typically a nonbank company that specializes in marketing to people with poor credit histories—dupes a homeowner into taking out a home equity loan or mortgage refinancing with unnecessary, excessive or undisclosed costs. Victims who have trouble repaying often face harassing collection tactics or are encouraged to refinance the loan at even higher fees. In the worst cases, people who can't repay end up losing their home. It's a problem known as "predatory" lending.

Examples of predatory practices

include schemes where the lender promises one type of loan or interest rate but switches to another one that's more costly to the borrower, and "equity stripping," in which the lender deliberately makes a loan that is beyond the borrower's ability to repay in hopes of foreclosing on the loan and taking possession of the house. Predatory lenders primarily target consumers they believe are vulnerable, such as older people who need money for medical bills or home repairs. "It's particularly tragic when an elderly borrower who takes such pride in the home he or she worked many long years to acquire loses it to a predatory lender," says Elizabeth Kelderhouse, a Community Affairs Officer with the FDIC.

***Best Defense:*** Beware of a letter or phone call from an unfamiliar lender or loan broker with what appears to be a fantastic offer to consolidate your debts or pay for new bills by refinancing your home. Think long and hard before taking out a loan where your home serves as collateral and can be lost if you can't repay. Talk to knowledgeable friends or professionals (perhaps your financial advisor or accountant) to discuss other options.

If you decide to get a home loan, contact several banking institutions or other reputable lenders, not just one, and try to negotiate the best deal. Walk away from a lender who refuses to put all costs in writing, dodges your requests to explain loan terms, tries to pressure you into quickly signing a contract or discourages you from allowing another person to review the contract before you sign. Don't agree to a loan contract if you don't understand the terms or conditions, dollar amounts or other key sections are left blank, there is information you know is false, there are unexplained changes in terms, or you feel you're being pressured to sign quickly. Remember that for certain loans secured by your home, the federal Truth in Lending Act gives you up to three business days after signing a loan contract to change your mind for any reason and cancel the deal without penalty.

If you obtain a home loan and you're having trouble making payments, get assistance as soon as possible so that you don't risk a foreclosure. For more tips and information about avoiding problems with predatory loans, read the Summer 2002 issue of ***FDIC Consumer News*** available online at www.fdic.gov/consumers/consumer/news or credit-related information on the FTC's Web site at www.ftc.gov/bcp/menu-credit.htm.

## Federal Laws Protecting You Against Fraud

**The Fair Credit Reporting Act (FCRA)** establishes procedures for correcting mistakes in your credit record, including unauthorized accounts. You have the right to receive a copy of your credit report for free if you suspect you are the victim of fraud. Your credit record may only be provided to people with a permissible need for the information (for example, a landlord or creditor) who must keep the details confidential.

**The Truth in Lending Act (TILA)** limits your liability if your credit card is lost or stolen. If someone uses your credit card without authorization, the most you are liable for is $50 in charges. (Financial institutions sometimes do not even ask for that much). If you dispute a charge on your card, the creditor has 90 days to resolve the matter, and you may withhold payment of the disputed amount during the investigation. For certain loans secured by your home, the TILA gives you three business days to cancel a contract without penalty—a big protection against a "predatory" home loan (see Page 6). **The Fair Credit Billing Act (FCBA)**, part of the TILA, provides other consumer protections if you withhold payment while disputing a credit card charge.

**The Electronic Fund Transfer Act (EFTA)** limits your liability for the unauthorized use of your ATM card, debit card or other device (not including credit cards) used in handling an electronic deposit, payment or withdrawal. If your ATM or debit card is lost or stolen, your liability under the EFTA is limited to $50 if you notify your financial institution within two business days of discovering the loss or theft. If you wait more than two business days to report a lost or stolen card but you notify the card issuer about an unauthorized transaction within 60 days of the date the bank mails the statement containing the error, you could lose as much as $500. If you wait longer than that, you may be liable for $500 plus the amount of any unauthorized transactions after the 60-day period. However, to promote the worry-free use of debit cards and ATMs, many financial institutions are voluntarily treating the fraudulent use of those cards as if they were credit cards—that is, a maximum liability of $50 per card, and sometimes less.

**Note**: No federal law limits your losses from check fraud, but you do have protections under state law. For example, most state laws hold the bank responsible for losses from a forged check, but they also require the bank customer to take reasonable care of his or her account, including monitoring account statements and promptly reporting an unauthorized transaction to avoid being liable for losses.

## Ten Simple Things You Can Do to Fight Fraud

**1. Protect your Social Security number, credit card and debit card numbers, PINs (personal identification numbers), passwords and other personal information.** A thief can use these details to order checks or credit cards, apply for loans or otherwise commit fraud using *your* name.

Among the preventive measures you can take: Don't provide financial and other personal information in response to an unsolicited phone call, fax, letter or e-mail—it could be from a fraud artist masquerading as a legitimate business person or government official. Be particularly cautious with your Social Security number (SSN). While your employer and financial institutions will need your SSN for tax purposes, you have the right to refuse requests for your SSN from merchants and service providers (who have other ways to identify you). Also, if your state puts SSNs on driver's licenses, find out if you can use another number.

Keep bank and credit card statements, tax returns, checks and other sensitive documents in a safe place at home. Shred these documents before discarding them.

Also choose PINs and passwords for your bank and Internet accounts that will be tough for someone else to figure out. Don't use your birth date or home address, for example. (More suggestions for guarding personal information appear elsewhere in this article and throughout our special report.)

**2. Deal only with legitimate, reputable businesses.** Try to do business with companies you already know or that have been recommended. Do your research before giving money or personal information to an unfamiliar merchant (or charity or any other organization). For example, contact your state's Attorney General's office or the Better Business Bureau and ask about complaints, lawsuits or other matters involving a company's reputation. To check out an unfamiliar banking institution, contact the FDIC (see Page 11).

**3. Get key details in writing and thoroughly check them out before agreeing to anything.** Don't rely on a sales person's oral representations for a significant purchase or investment. Get as much written information as possible, including a contract, specifying cost information and your consumer rights. If a marketer refuses to supply written information or employs high-pressure sales tactics to get you to act fast, take that as your cue to say "goodbye."

**4. Beware of "deals" requiring money up-front.** "Congratulations, you've won a free vacation!" "Get rich quick-at no risk!" "We'll fix your credit problems—fast." Do these sound familiar? They're likely to be schemes to trick you into sending money or providing bank account information in exchange for promises of goods or services that will never be delivered. Be skeptical of any offer that's "free" or otherwise hard to believe and that, as a precondition, requires you to pay money (perhaps for a supposed "fee" or "tax").

**5. Be extra careful when providing personal information over the telephone or Internet.** Scam artists hide at the other end of the phone line or computer screen. So, don't give bank account information, Social Security numbers or personal data in response to an unsolicited phone call or e-mail. Remember that a legitimate company would never ask for passwords or other personal information by e-mail. Before providing credit card or other information to a Web site, confirm that the site is legitimate, not a copycat designed by a crook, by verifying that the Web site's address is an exact match for what appears in literature from the company or some other reliable source. You'd be wise to avoid an online merchant that doesn't list a phone number or physical address—possible signs that the Web site and its owners are fraudulent. Also look for assurances on the Web site about security procedures for safely transmitting and storing your credit card number, password and other personal information you're asked to provide.

**6. Safeguard your incoming and outgoing mail.** It could include checks, credit card applications, bank statements and other items of value to a thief. Try to send and receive mail using locked mailboxes or otherwise secure locations. Remove incoming mail from your mailbox as soon as possible. If your mailbox is unlocked and you're going to be away on vacation or some other travel, have your mail held at the post office or picked up by a neighbor. If you're expecting a check, a

credit card or bank account information and it doesn't arrive in a reasonable period, notify the sender. As for outgoing mail containing a check or other personal financial information, put it in a blue Postal Service mailbox, hand it to a mail carrier or take it to the post office.

**7. Stop bandits from recycling your trash into cash.** Thieves known as "dumpster divers" pick through garbage looking for credit card applications, monthly bank statements, receipts, "loan checks" (mailed by financial institutions with offers to "write yourself a loan") and other documents they can use to commit fraud. Before tossing out these items, destroy them, preferably using a "crosscut" shredder that turns paper into confetti. Before selling, donating or disposing of an old personal computer, use special software to completely erase files that contain financial records, tax returns and other personal information. Also, "Be aware that thieves can sometimes access personal information from computer disks, even if you've deleted or revised the files on the disk," warns Elizabeth Kelderhouse, an FDIC Community Affairs Officer. "The easiest solution is to break any disk before throwing it away."

**8. Limit the confidential information in your wallet in case it gets lost or stolen.** Don't carry around more checks, credit cards or other bank items than you need. Consider reducing the number of credit cards you carry by canceling ones you don't use. Keep passports, Social Security cards and birth certificates in a secure place, not in your wallet. Never keep passwords or PINs on or near your checkbook, credit card, ATM card or debit card.

**9. Review your credit card bills and bank statements as soon as they arrive.** If you notice something suspicious, perhaps a credit card purchase you didn't make or an unauthorized withdrawal from your checking account, contact your financial institution immediately. While federal and state laws limit your losses if you're victimized by a financial fraud, sometimes your maximum liability depends on how quickly you report the problem (see Page 7). Also make sure you get your statement every month. If no statement arrives, that could be a sign that an identity thief has changed your mailing address for purposes of committing fraud in your name but from another location.

**10. Monitor your credit report for warning signs of fraud.** Most experts say you should check your credit report at least once a year from each of the three major credit bureaus: Equifax (800-685-1111, www.equifax.com); Experian (888-397-3742, www.experian.com) and TransUnion (800-888-4213, www.transunion.com). A copy of your credit report is free in some states and some situations (such as if you believe you're a fraud victim or if you were recently denied credit or a job based on a credit report), but the most you'll pay under current rules is $9. When you get your report, look for anything suspicious, such as credit cards and loans or leases that have been wrongfully taken out in your name. Another option is to pay a service to help you monitor your credit report for possible signs of fraud (see next page).

## For More Information About Fighting Fraud

**The FDIC and the other federal banking regulators** listed on Page 11 have publications, Web sites, staff and other resources that can help answer your questions. For example, you can read articles about financial frauds in past issues of ***FDIC Consumer News*** at www.fdic.gov/consumers/consumer/news. The FDIC also has developed an adult financial education program called "Money Smart" that is designed to help banks and other organizations teach basic money management skills, including some that can be effective in avoiding fraud. For more details, go to www.fdic.gov/consumers/consumer/moneysmart.

**The Federal Trade Commission** works to prevent fraudulent, deceptive and unfair business practices and to provide helpful information to consumers. To file a complaint or to get free information, visit www.ftc.gov or call toll-free 877-FTC-HELP (1-877-382-4357). The FTC also maintains the U.S. government's central Web site for information about identity theft (www.consumer.gov/idtheft).

**Other consumer information is available from the federal government,** including news and alerts about scams and frauds posted on the Web site of the Federal Citizen Information Center (FCIC) at www.pueblo.gsa.gov/scamsdesc. Also call the FCIC for fraud-related publications (toll-free 888-878-3256).

# Paying Extra for ID Theft Protection? Consider Costs vs. Benefits

The private sector is promoting new products to help people detect identity theft or cover certain losses. But are these products right for you? ***FDIC Consumer News*** can't endorse or recommend a particular product, but we can give you information to help you decide for yourself. Here we focus on two common products being marketed.

## CREDIT REPORT MONITORING

As we noted on Page 9 of this issue of ***FDIC Consumer News*** and in our special report on credit records in the Winter 2002/2003 edition, most experts recommend that you get a copy of your credit report at least once a year from each of the three major credit bureaus (Equifax, Experian and TransUnion) to ensure the report's accuracy and to look for signs of ID theft (such as a credit card account opened or requested by a con artist using your name). You can order a copy of your credit report directly from each major credit bureau for a maximum charge of $9 per report (free in some states or situations). But consumers also can subscribe to a monitoring service offered by credit bureaus or other companies for about $30 to $150 a year, depending on what's included.

A monitoring service may provide, for example, an automatic copy of your credit report from one credit bureau or all three major companies, perhaps on a quarterly or monthly basis. You also may be able to get e-mail notices of any changes in a credit report, even within 24 hours. "The most important alert is one telling you that an account has been opened in your name," says Robert Patrick, an FDIC attorney. "If you do not recognize it as your account, you can take immediate action to get the account closed. Otherwise, you may not hear about accounts opened by an identity thief for months."

Should you order credit reports on your own or pay more for a special service? The answer depends on how closely you want to monitor your credit reports and how much you are willing to pay for convenience or other extras. Some consumer advocates and other observers say that most people would be adequately protected if they order their own credit reports from the three major credit bureaus at least once a year and save money over the cost of a professional monitoring service. The nonprofit Identity Theft Resource Center in San Diego offers this strategy: stagger your requests throughout the year—"for example, Experian in the beginning of January, TransUnion in April, Equifax in August."

If you want to stay on top of your credit history but don't have the time or desire to submit periodic requests on your own (even once a year), you may want to consider paying a monitoring service, preferably one covering all three major credit bureaus.

## IDENTITY THEFT INSURANCE

If an ID thief uses your name to commit fraud you are likely to incur expenses— sometimes hundreds or thousands of dollars—in correcting your credit files or otherwise defending yourself. That's why some insurance companies now sell ID theft insurance, and other companies, including some credit card issuers, will be offering the protection soon. The policies typically cover expenses such as lost wages while you take time off from work to fix problems; fees associated with reapplying for loans you were denied; and the costs of mailings and phone calls to creditors, credit bureaus and law enforcement agencies. The policies also may cover certain legal fees, which can be significant. The policies do not, however, cover losses for which you are liable by law or that are otherwise not reimbursed by a financial institution or merchant.

You may already have this insurance at no extra charge through your homeowner's insurance or your credit card. Or you may be able to buy the coverage separately for about $25 a year or more. The insurance generally includes a deductible (cost to you) of $100 to $250 per claim. If you're thinking about buying a policy, consider the annual insurance costs vs. the amount you'd probably recover if you were to become an ID theft victim. Also get an opinion from someone knowledgeable, perhaps your financial planner or an insurance professional you trust.

***Important:*** Beware of telephone or Internet scams promoting credit monitoring services, "free" credit reports, or credit card or ID theft insurance. These frauds typically use false or misleading statements to get you to send money or divulge personal information, including credit card or bank account numbers. Protect yourself by following our tips on Page 8 about how to avoid fraudulent offers.

# For General Information

The **Federal Deposit Insurance Corporation** insures deposits at banks and savings associations and supervises state-chartered banks that are not members of the Federal Reserve System. The FDIC's services include a toll-free consumer assistance line, answers to written questions, and informational material. Toll-free phone: (877) ASK-FDIC or (877) 275-3342. The phone line is staffed Monday through Friday, 8:00 a.m. to 8:00 p.m., Eastern Time. Recorded information is available 24 hours a day. The toll-free TTY number for hearing-impaired consumers is (800) 925-4618. Home Page: www.fdic.gov. Mail: 550 17th Street, NW, Washington, DC 20429.

**For questions about deposit insurance coverage:** Contact the FDIC Division of Supervision and Consumer Protection at the address and phone numbers above, by fax to (202) 942-3098, or by e-mail using the Customer Assistance Form on the Internet at www2.fdic.gov/starsmail/index.html. The National Credit Union Administration (listed below) insures deposits at federally insured credit unions.

**For other questions, including those about consumer protection 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. Other regulators are listed below. To submit a complaint about an FDIC-supervised institution, contact the FDIC Division of Supervision and Consumer Protection as listed above. For inquiries involving problems or complaints related to the FDIC, contact the FDIC Office of the Ombudsman at the mailing address and phone numbers listed above, by fax to (202) 942-3040, or by e-mail to ombudsman@fdic.gov.

The **Federal Reserve System** supervises state-chartered banks that are members of the Federal Reserve System. Phone: (202) 452-3693. Fax: (202) 728-5850. Home Page: www.federalreserve.gov. Mail: Division of Consumer and Community Affairs, 20th Street and Constitution Avenue, NW, Washington, DC 20551.

The **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.) Phone: (800) 613-6743. Fax: (713) 336-4301. Home Page: www.occ.treas.gov. E-mail: consumer.assistance@occ.treas.gov. Mail: Customer Assistance Group, 1301 McKinney Street, Suite 3710, Houston, TX 77010.

The **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.) Phone: (800) 842-6929 or (202) 906-6237. Home Page: www.ots.treas.gov. E-mail: consumer.complaint@ots.treas.gov. Mail: Consumer Affairs Office, 1700 G Street, NW, Washington, DC 20552.

The **National Credit Union Administration** charters and supervises federal credit unions, and insures deposits at federal credit unions and many state credit unions. Phone: (703) 518-6330. Fax: (703) 518-6409. Home Page: www.ncua.gov. E-mail: pacamail@ncua.gov. Mail: Office of Public and Congressional Affairs, 1775 Duke Street, Alexandria, VA 22314.

**Your state government** also may offer assistance and publish useful information. Contact your state's Attorney General's office, consumer protection office or financial institution regulatory agency as listed in your phone book or other directories, or visit your state's official Web site.


## FDIC *Consumer News*

Published by the Federal Deposit Insurance Corporation

**Donald E. Powell**, *Chairman*

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

**Elizabeth Ford**, *Assistant Director*, OPA

**Jay Rosenstein**, *Senior Writer-Editor*, OPA

**Tommy Ballard**, *Illustration*

**Mitchell Crawley**, *Graphic Design*

***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, Editor, ***FDIC Consumer News***
550 17th Street, NW
Room 7100
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
Toll-free phone: (877) 275-3342 or (202) 416-6940 (Washington area)
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. To receive e-mail notification of new issues, with links to stories, write to listserv@peach.ease.lsoft.com and type "Subscribe FDIC-consumernews" (include the hyphen) and your name in the message area.

# A Final Exam on Financial Fraud

## Test your knowledge by taking our quiz based on information in this issue

**1.** Identity theft (when a swindler uses someone else's name to obtain credit cards or loans that won't be repaid) is, by far, the top fraud complaint reported to the Federal Trade Commission. ***True or False?***

**2.** If you receive an e-mail saying a computer malfunction has occurred at a company you do business with (perhaps your bank or Internet service provider), and you're asked to "re-enter" your Social Security number and bank account information to help restore the missing records, it's safe to provide this information as long as the e-mail correctly identifies the company's name. ***True or False?***

**3.** A thief steals a pre-approved credit card application from your trash or mailbox. He or she then may be able to order a new credit card in your name and have it mailed to him or her at a different address. ***True or False?***

**4.** Under federal law, if a crook uses your credit card to go on a spending spree, you are liable for up to $50 of the fraudulent charges. But if a thief uses your ATM card or debit card, you could be responsible for $500 or more in unauthorized transactions. ***True or False?***

**5.** If a con artist posing as a legitimate businessman instructs your bank to electronically transfer money from your checking account, you are not liable for any loss if you notify your bank within 60 days of the date the bank statement containing the error is mailed to you. ***True or False?***

**6.** If you're selling an item on the Internet or through an ad in your local paper, it's always safe to accept a cashier's check as payment because a cashier's check, unlike a personal check, cannot be counterfeited. ***True or False?***

**7.** Your credit report may reveal that you have been a victim of fraud, such as credit cards and loans or leases that have been wrongfully taken out in your name. ***True or False?***

*Correct answers:*

1. True (See Page 2)
2. False (See Page 6)
3. True (See Page 4)
4. True (See Page 7)
5. True (See Page 6)
6. False (See Page 4)
7. True (See Page 9)

Federal Deposit Insurance Corporation
Washington, DC 20429-9990

OFFICIAL BUSINESS
Penalty for Private Use, $300

PRESORTED
STANDARD
MAIL
Postage & Fees
Paid FDIC Permit
No. G-36