FDIC Consumer News - Fall 1997

FDIC Consumer News is published by the Federal Deposit Insurance Corporation
Andrew C. Hove, Jr., Chairman
Phil Battey, Director, Office of Corporate Communications
Elizabeth Ford, Assistant Director, Office of Corporate Communications
Jay Rosenstein, Senior Writer-Editor
Tommy Ballard, Graphic Design and Illustration

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

See other issues of FDIC Consumer News online.

To receive e-mail notification of the 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.

Other consumer information on the Internet is available from the FDIC at www.fdic.gov.

Comments, suggestions or questions may be sent to: Jay Rosenstein, FDIC, 550 17th Street, NW, Washington, DC 20429, E-mail or Fax (202) 898-3870.

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

Last Updated 08/03/1999 communications@fdic.gov

Your Wallet: A Loser's Manual

A thief who takes your wallet can steal your identity, too, and use your good name to run up big bills. Here's how to protect your money and your credit record and your sanity if your wallet is lost or stolen.

Consider this: Your wallet is stolen. You immediately call your bank and credit card company to report the problem, close old accounts and open new ones. You feel fairly confident that the incident is behind you.

But a few weeks later you receive a threatening notice to pay a "past-due" bill for some merchandise you know you never purchased. Next, your application for an auto loan gets rejected because of a poor credit history, when you know you never missed a loan payment or bounced a check in your life. Shocked, you immediately call one of the major credit bureaus (also called a credit reporting agency), which informs you that numerous accounts have been opened, using your name and Social Security number, and with thousands of dollars in debts to stores, credit cards, utilities and other companies. The good news: Your actual liability for these unauthorized purchases is limited by law or industry standards. The bad news: You still spend many frustrating hours trying to clear your name and straighten out your credit history.

Sound like fiction? It's not. It could happen to you any time, anywhere. We're talking about "identity theft"- situations where a con artist obtains charge cards or enough personal information to establish new accounts in your name.

"Most of us assume that thieves are interested in cash when they steal a wallet, but in many cases the cash may be the least valuable item," says Pete Hirsch, a fraud examiner with the FDIC's Division of Supervision in Washington. "Your wallet can provide a criminal with ready access to sensitive information that can be used to steal your identity, drain bank accounts and make it difficult for you to obtain credit in the future."

Identity theft is on the rise in the United States and, unfortunately, many consumers don't know how to adequately protect themselves or the contents of their wallets. People too often assume that when a wallet is lost or stolen they simply need to cancel their "plastic" (credit, debit, and ATM cards) and replace lost identification. But there are other steps, including some preventive measures, that you can take to greatly reduce your chances of becoming a victim.

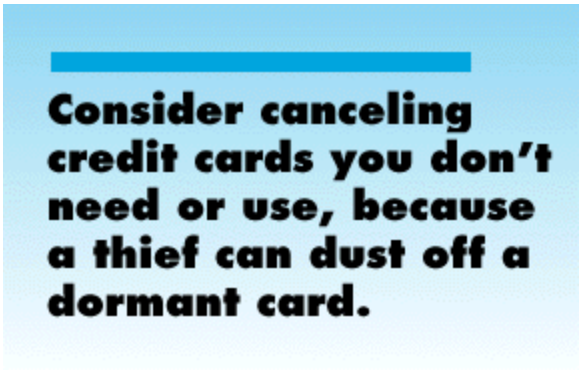
Here's a collection of tips and information from FDIC Consumer News that we think can help you protect against all kinds of financial fraud, even if you never lose your wallet. Remember: A con artist doesn't need to steal your wallet to steal your money and your identity. A sophisticated thief simply needs a little information about you - perhaps one of your credit card numbers or your Social Security number - to make purchases or obtain new accounts in your name. So some of the suggestions in this report can help.

Preventive Measures

One simple way to protect yourself against identity theft is to limit the amount of confidential information you carry in your wallet. Experts recommend that you not carry around bank account numbers, personal identification numbers (PINs), passports, birth certificates, and most importantly, Social Security cards. (Although many states continue to use Social Security numbers on drivers' licenses, this practice is changing.)

Avoid carrying more blank checks than you really need. Not only can a thief cash checks or use them for purchases, but a crook also can make use of the sensitive information often pre-printed on your checks (your address, bank account number, even your telephone number). Many consumers even print their driver's license number or Social Security number on their checks. That's a definite no-no, because either number could help a thief apply for a loan, credit card or bank account in your name.

Keep good backup information about your accounts, just in case your wallet is lost or stolen. You'll want account numbers and phone numbers that can be used to report your losses or request new cards or emergency cash. Some people recommend photocopying your credit, debit, and ATM cards, as well as your driver's license and passport information. Another approach is to simply list key numbers on a handy sheet of paper, and we've given you a start with our checklist.



"Keep these numbers in safekeeping or else they can become tools for someone with criminal intent," says Deirdre Foley of the FDIC's Division of Compliance and Consumer Affairs in Washington. You'll also want ready access to these papers, too. That's why a safe deposit box or other restricted area might not be a good storage place for these numbers in case you need immediate access at night or on a weekend or holiday.

If you're going on vacation, Ken Baebel, also from the Division of Compliance and Consumer Affairs, recommends taking along a list of the toll-free telephone numbers for your banking and credit card companies not your card numbers and keeping the list in a safe place other than your wallet. "If you lose your wallet while you're away from home, having those phone numbers will help you quickly report the problem and get replacement cash or cards," he says.

Why not take a list of card numbers with you on your trip? "The card numbers alone can be just as valuable to a thief as the actual cards themselves, if not more valuable," explains Gene Seitz, a fraud investigator in the FDIC's Division of Supervision in Washington. "If someone steals your wallet, you'll probably notice that right away. But if someone steals a list of card numbers from your suitcase, you might not be so quick to realize that, and that just gives the thief more time to run up fraudulent charges."

Consider canceling any credit cards you don't really need or use. Among the reasons: A thief can dust off a "dormant" card and use card numbers and other personal information to make purchases or get a new card. You'll only find out about the problem when the collection notices arrive at your address.

Never give out personal information (such as your Social Security number, credit card numbers or your address) over the telephone unless you initiate the call, and it's to a well-known and trusted outfit. Also try not to provide personal information when using a check or plastic for purchases at a cash register. Many states even prohibit merchants from requiring personal details.

Don't just toss away those credit card applications you receive in the mail and don't intend to apply for. Shred them as best you can. Crooks can easily use these applications to establish accounts in your name and then change the mailing address so you're unaware of the fraud until it's too late. Also, if you don't want to receive unsolicited credit card applications in the mail, by law you can demand that your name be removed from the marketing lists that credit bureaus sell to credit grantors looking for new customers. To "opt out" of these mailings, call any one of the following credit bureaus at these toll-free numbers specifically established for this purpose: Equifax at (800) 556-4711, Experian at (800) 353-0809, or Trans Union at either (800) 241-2858 or (800) 680-7293.

Review your credit card bills and your checking account statements as soon as they arrive, to ensure that no fraudulent activity is taking place. Also make sure you get a statement from your creditors every month. If no statement arrives, that could be a sign that someone has changed your billing address for fraudulent purposes. And, finally, periodically request a copy of your credit report and check for signs that someone has opened accounts in your name. The three major credit bureaus and their toll-free numbers for requesting copies of your credit report are: Equifax at (800) 685-1111, Experian at (800) 682-7654, and

Trans Union at (800) 888-4213. If you've been denied credit, you may be entitled to a free copy of your report. If you haven't been denied credit, the most you can be charged is $8.

While it may seem obvious, it can't hurt to mention a few basic words about protecting your wallet: Don't take out your wallet until you actually need it, and don't forget your wallet before leaving a restaurant, store or any public place. And never put your wallet down alongside a cash register, in a phone booth or even on top of your car. A good rule of thumb, as we've noted previously in FDIC Consumer News, is this: Never set down your wallet unless your hand is attached to it.

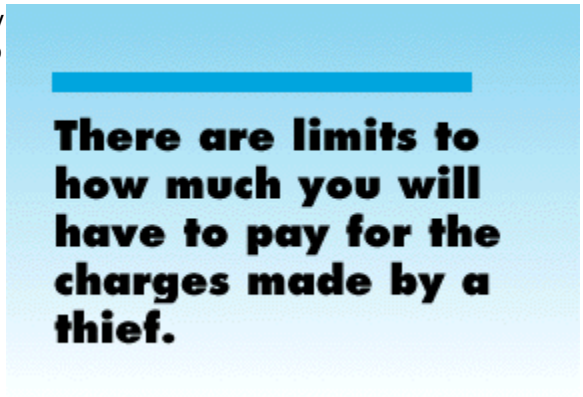
Know Your (Liability) Limits
A brief overview of your potential liability when victimized by credit card or banking fraud.

If You've Already Been Victimized

If your wallet disappears, there are limits to how much you will have to pay for the charges made by a thief (see the article Know Your (Liability) Limits). In some cases you may owe nothing. But you can help limit your liability and reduce potential losses for merchants and banks (which often get passed on to consumers in the form of higher costs for goods and services) by doing the following.

First, immediately call your credit and charge card companies on their toll-free numbers and explain the situation. You may not have to pay for fraudulent charges if you notify the card issuer quickly (usually within two business days of discovering the loss or theft).

Instruct your card companies to close your accounts. Why close them instead of just asking for fraudulent charges to be removed? For one thing, it'll be difficult for the card issuer to identify and prevent all fraudulent purchases. Also, it's good to have your credit reports show that an account was "closed at customer's request" instead of "lost or stolen." The latter could indicate that you somehow were at fault. And follow up your phone conversations with letters to the card companies - to ensure an adequate "paper trail." It may help to keep a detailed log of phone calls and letters to avoid confusion and to prove that you made the required notifications.



After you've closed your credit card accounts, open new ones with new account numbers and PINs. Replace your old ATM card with a new one, and change your existing PIN to one that cannot be easily guessed by a thief. Your birth date and portions of your Social Security number, telephone number or street address usually are poor choices for PINs.

Canceling your credit card may not be enough to stop crooks from applying for new accounts. That's why you also should contact the three big credit bureaus and have them "flag" your file as one belonging to a possible fraud victim. (See the guide on the previous page.) This warning will caution credit grantors to check with you before approving new loans or cards in your name. Experts say you should take the time to call all three credit bureaus, and perhaps even follow up in writing.

Immediately notify local police where the wallet was lost or stolen. Hugh Eagleton of the FDIC's Division of Compliance and Consumer Affairs recommends that you fill out a police report and ask about signing a

written affidavit verifying that unauthorized transactions in your name are fraudulent. "These documents will help you when dealing with your bank or credit card company or removing clouds from your credit record," he says. "They give you more credibility when you say that you had no part in any fraud."

Also worth calling: the Social Security Administration (for replacement of Social Security and Medicaid cards), the Department of Motor Vehicles (to get a new driver's license), and your telephone and utility companies (to prevent a con artist from using a utility bill as proof of residence when applying for new credit cards).

Final Thoughts

There's no doubt about it: Our recommendations are time-consuming. But victims of lost wallets and identity theft can tell you that the extra efforts we've described would be far preferable to the many hours you would spend trying to erase a criminal's fingerprints from your credit record. Remember: Your name and good credit history are among your most valuable assets. Protect them.

Don't Lose These Names and Numbers

Fill out this personal guide and keep it in a safe place. If your wallet is lost or stolen you'll know who to call and what to say. When traveling, take along a similar list, but don't include account numbers or expiration dates.

Checking Accounts
Immediately call to cancel checking accounts and start new ones.

Institution name - Toll-Free Phone - Account Number -

Credit Cards and Other "Plastic"
Immediately cancel credit, debit, ATM and other cards, but ask for replacements.

Card 1	Institution Name - Toll-Free Phone - Account Number - Expiration Date -
Card 1	Institution Name - Toll-Free Phone - Account Number - Expiration Date -
Card 1	Institution Name - Toll-Free Phone - Account Number - Expiration Date -

Law Enforcement
Immediately call to report a lost or stolen wallet and ask about filing an official report.

Police -

Credit Bureaus
Call all three major credit bureaus' fraud departments to spot thieves from opening new accounts in your name.

Equifax - *Fraud unit phone number available from your creditor or the police.* Experian - **(800) 301-7195** TransUnion - **(800) 680-7289**

Miscellaneous Identification
Call to report a lost Social Security/Medicaid card, driver's license, passport and other items.

Social Security Administration - **(800) 772-1213** Department of Motor Vehicles - U.S. State Department regional Passport Agency -

Know Your (Liability) Limits

The Electronic Fund Transfer Act and the Fair Credit Billing Act are among the federal laws protecting consumers from liability if they've been victimized by credit card or banking fraud. In many cases your liability is limited to the first $50 of loss, but that depends on the type of account and how quickly you report the problem. Here's a brief overview of what you should know about your potential liability.

Automated Teller Machine (ATM) Cards: If a thief withdraws money from a cash machine using your ATM card, your maximum liability is $50 if you report your card lost or stolen within two business days of discovering the loss (not within two days of the transaction). If you report the loss within 60 days, your maximum exposure is $500. Wait more than 60 days and you could be liable for all the money the thief obtained using your ATM card, plus other charges, such as fees for bounced checks.

Checks: State laws govern whether you'd be held responsible if a lost or stolen check were used in a forgery. In most cases you probably won't be held liable for losses. However, bank customers generally are responsible for paying "reasonable" attention to their accounts and for protecting them against misuse. "A bank may refuse to reimburse you for a forged check if it believes you were negligent," says FDIC attorney Mark Mellon. "Negligence may include failing to safeguard your checks, filling them out in a way that would be easy to alter, or not notifying the bank about a loss in a timely manner." Among the ways to protect yourself: Look at your bank statement within a month of receiving it and immediately notify the bank of any suspicious or unauthorized transactions.

Credit Cards: Under federal law, the most you'd owe for unauthorized charges to your credit card is $50 per card. You owe nothing if you report the problem before charges are made.

Debit Cards: These cards can be used to pay for purchases out of your checking account but without writing a check. There are two types of debit cards - an "on-line" card that requires a personal identification number (PIN), and an "off-line" card where no PIN is needed as an ID. Many consumers think of a debit card (and its liability) as being comparable to a credit card because both can be used at cash registers or to order products over the phone. Until recently, however, consumer liability for a lost or stolen debit card was comparable to an ATM card (see left), which may be far higher than that of a credit card ($50 maximum loss). Consumer groups and members of Congress complained about off-line cards in particular because, without requiring a PIN, these cards are more susceptible to fraud. VISA and MasterCard recently announced voluntary changes that currently put your maximum loss from a missing debit card at $50, the same as for credit cards. Contact your card issuer for more details. Legislation also is before Congress that would impose this same $50 limit by law, to ensure the continuation of this protection.

Stored-Value Cards: These cards are loaded with a set dollar value and can be used to pay for small-dollar purchases. A stored-value card essentially is electronic cash. Accordingly, your loss is equal to the amount of money on the card.

Basic Points About the Most Basic Type of Insured Deposit - the Individual Account

The individual or single-ownership account is the most basic type of deposit held by consumers at FDIC-insured banks and thrifts. In its simplest form, it's a checking or savings account owned by just one person. But even with a basic account, it's important to make sure your funds are within the $100,000 insurance limit, just in case your institution fails. To help answer some of the most common questions about individual accounts, ***FDIC Consumer News*** provides the following list of key points.

Point #1: ***Your individual accounts are protected to $100,000 separately from other types of accounts you own at the same institution.*** In other words, your individual accounts and the interest they've accrued qualify for a combined $100,000 of FDIC insurance at an institution, separate from your joint accounts, retirement accounts and certain business and "payable-on-death" accounts. We'll give more specifics later.

Point #2: ***To qualify as an individual account for insurance purposes, it must be owned by one person.*** It cannot be one account owned by two or more people, or by a corporation or partnership.

Point #3: ***If you are the sole proprietor of a business, your business accounts are insured together with your individual accounts under the same $100,000 ceiling.*** A sole proprietorship is a business owned by just one person rather than a corporation or partnership. Many small stores or service companies function as sole proprietorships. If you have a sole proprietorship, your personal and business accounts at the same institution would be insured together as individual accounts up to $100,000 in total, not separately for a combined $200,000. On the other hand, if you own a corporation or partnership, your personal deposits are not counted with your business accounts for insurance purposes.

Point #4: ***You may give another person the right to withdraw money from your deposit account, but be careful not to reduce your insurance coverage.*** Many consumers are smart to want a loved one to have access to their funds in an emergency or otherwise. But they sometimes change an account without thinking of the implications, including the possibility of reducing their overall coverage at any one bank or thrift. In general, if more than one person can withdraw from an account, it is considered a joint account. However, if you give another person a "power of attorney" to withdraw funds from your account, the FDIC will consider this an individual account, not a joint account. Similarly, if you clearly indicate in the bank's records that the funds are owned solely by you but that you authorize another person to withdraw from the account on your behalf, as a convenience, the FDIC will consider this your individual account, not a joint account. Why does that matter? If you don't understand the rules, you inadvertently may be creating joint accounts and therefore putting some of your money, or your loved ones', over the $100,000 insurance limit for joint accounts.

Point #5: ***Know the rules for deposits held on behalf of someone else.*** For example, the funds of an estate that are deposited by an administrator are added together with any other funds the deceased person had at the same institution and insured up to $100,000. Also, a deposit account for a youngster under the Uniform Gifts to Minors Act (i.e., the parent or guardian still maintains limited control over the funds) is insured to $100,000 as the minor's individual account, not as an account owned by or with the adult. (For information about the coverage of "payable-on-death" or "revocable trust" accounts, see the spring 1995 edition of ***FDIC Consumer News***, available from the FDIC's Public Information Center listed on the front page.)

"The FDIC knows that some of the rules for individual accounts can be confusing, even to a banker," says Joe DiNuzzo, a senior counsel in the FDIC's Legal Division. "We also know that every question or concern is important when it's your money at stake." That's why the FDIC has a booklet, "Your Insured Deposit," which provides additional information on individual accounts and other types of deposits. You can get a copy of this booklet free of charge at your local bank or thrift, as well as from the FDIC's Public Information Center and our Internet site (www.fdic.gov). Or, call or write the FDIC's Division of Compliance and Consumer Affairs (see For More Information) for answers to specific questions.

Internet Banking and Shopping: Cyber-Buyer Beware

Here are tips to help you avoid online problems and scams

As the Internet continues to expand, more banks are offering customers the ability to transfer funds, view account information, pay bills and conduct other transactions over the 'Net. In addition, other companies are offering customers the ability to shop online.

While "cyberbanking" and "cybercommerce" offer great convenience, they can be sources of concerns for consumers. The FDIC is aware of a few problems and pitfalls in particular, including:

- Companies pretending to be banks offering unusually high interest rates on deposits that, in reality, are not banks and are not insured by the FDIC;
- Thieves using sophisticated computer programs to obtain sensitive information, such as credit card or Social Security numbers, when consumers pay for purchases over the Internet or send e-mail to friends;
- Get-rich-quick schemes and fraudulent investment opportunities appearing on the Internet; and
- People or companies collecting information about the buying habits or interests of consumers
  who visit their Internet sites, and then selling that information to other companies - resulting in unwanted e-mail solicitations.

How can you protect yourself when banking, investing or shopping online? Here are tips from Jeffrey Kopchik, an attorney in the FDIC's Office of Policy Development in Washington who specializes in electronic banking and commerce, and Cynthia Bonnette, the chairman of an FDIC task force on new banking technologies.

Guard against a bogus Internet site: Be skeptical about an Internet site claiming to be a bank that offers interest rates on deposits significantly above what other banks are paying. Also be skeptical if the advertisement is offering any other deal that seems too good to be true (such as tax-free deposit accounts) because it probably is too good to be true!

Kopchik says that before depositing funds in a bank that advertises or transacts business on the Internet, make sure the institution has been legally authorized to do banking business. You can find that out by calling your state banking department (usually listed in your local phone book) or any of the federal banking regulators noted in the For More Information section of this newsletter. "Some entities operating on the Internet aren't banks even if the word 'bank' appears in their name or they describe themselves as a bank," Kopchik notes. "Two uninsured entities falsely claiming to be Internet banks were Freedom Star National Bank and Netware International Bank; both were recently shut down by authorities."

Consumers who send money to a bogus bank run the risk of losing their funds when the people who created it shut down the operation and disappear with the money. Consumers also should be aware that other types of financial services companies and some foreign banks operating Web sites are not FDIC-insured. People who send money to those institutions won't get their funds back from the FDIC if the company closes. A recent example of a foreign bank on the Internet that closed and caused losses was the European Union Bank based in the West Indies.

You also can find out if a bank's deposits are federally insured by calling the FDIC's Division of Compliance and Consumer Affairs toll-free (see details in the For More Information section of this newsletter) or by consulting the Institution Directory on the FDIC's Internet home page. Be aware that some legitimate banks operate on the Internet using trade names that differ from the legal name of the institution. When in doubt, your best bet is to call the FDIC.

Before purchasing goods or services over the Internet: Try to find out if anyone you know has dealt with the merchant online and ask how it went, Kopchik says. If you don't have personal references for the merchant, consider asking for guidance from your local Better Business Bureau or Chamber of Commerce. Both the U.S. Chamber of Commerce and the American Institute of Certified Public Accountants have indicated that they have plans to "certify" merchants who do business over the Internet. Some Internet service providers vouch for merchants that operate from their sites. For example, America Online will cover your maximum loss from credit card fraud ($50 per card under federal law), provided you report the fraud promptly.

Be careful using your credit card number when buying over the Internet. Most reputable merchants who accept card payments over the Internet use a system that scrambles or "encrypts" your card number so it can't be read by outsiders. The latest version of some popular Internet browser programs (such as Netscape Navigator and Microsoft Internet Explorer) may be equipped with encryption technology. Your computer screen generally will display some sort of logo (for example, a "lock and key") showing that your message is being encrypted. The major credit card associations (VISA and MasterCard) also have announced plans to start a new system they say will safely transmit credit card numbers over the Internet and verify the authenticity of merchants.

Some merchants may encourage you to pay electronically without using your credit card number. Perhaps you'll be asked to maintain an "electronic wallet" with a company (CyberCash is one) that will pay the merchant on your behalf. In other cases, companies will enable you to pay a merchant using your credit card but without transmitting the card number over the Internet.

Finally, if you think you've been victimized by a fraud, contact the Internet Fraud Watch of the National Fraud Information Center, which forwards reports of suspected crimes to federal and state authorities. Its toll-free number is 800-876-7060, and its Internet site is www.fraud.org. Or, you can report the suspected fraud directly to the appropriate federal or state agency (for example, the Securities and Exchange Commission if the company is a stockbroker).

Privacy on the Internet: As you spend time on the Internet, the various Web sites you visit may collect information about you, with or without your knowledge, regarding such things as the kinds of products you buy and the topics you find interesting. These Web sites may use this information internally or sell it to other firms or organizations. While these practices are not illegal, they may result in unwanted e-mail from unfamiliar companies or groups.

"Look to see if a Web site you are visiting discloses the company's policy about collecting and using the information it gathers," says the FDIC's Bonnette. "If it doesn't disclose its policy and you want to know more, follow up by calling or e-mailing the company." Among your other options: software from Internet service providers and computer stores that can block unwanted e-mail.

Final Thoughts

While the Internet has made it possible to bank, invest and shop from the comfort of your home, you still have to be cautious. After all, just because you "surf" the Internet you don't want a thief to "wipe out" your money.

Keeping the Costs of "Loan Checks" in Check

Lenders are mailing checks that enable consumers to write themselves a loan. But this convenience may come with a high price and other potential perils.

You've probably received checks in the mail from banks and other financial institutions offering you the chance to write yourself a loan, perhaps for up to $10,000 or more. For many people, a "loan check" - also known as a "convenience check" or a "live check" - is a convenient way to buy merchandise, pay bills, obtain cash or transfer a balance from one loan or credit card to another. The convenience comes from not having to leave your house or fill out a lengthy application to get the loan. But according to Pete Hirsch of the FDIC's Division of Supervision in Washington, "many consumers don't realize the potential risks of loan checks, including high costs and the possibility of the

checks being used by criminals." These and other concerns have prompted recent congressional hearings as to whether unsolicited mailings of loan checks should be banned. To help you learn more about the potential risks of loan checks, FDIC Consumer News offers the following guidance.

Understand the Costs

By signing or cashing a loan check, you are agreeing to all the terms and conditions of a loan you must pay back. That's why it's important to first check the interest rate, which may range from the low-teens to as high as the mid-twenties. Loan checks also carry other expenses, including substantial fees. In addition, you may not be allowed a "grace period" - interest charges would begin accumulating as soon as you use the loan check. Because of these costs, we suggest that you thoroughly read the literature sent along with the blank checks so that you are aware of all charges. If you have any questions, contact the issuer before using these checks. Many consumers may find they're better off simply writing a standard check from their account, using a debit card or charging purchases.

Protect Against Fraud

Fraudulent use of loan checks is fast becoming a serious problem for bankers, merchants and law enforcement authorities. In general, loan checks mailed to consumers are relatively easy for thieves to identify and to steal (from mailboxes or elsewhere). The fact that most loan checks were never requested by the intended recipient means that the consumer may be unaware a check was stolenuntil the bills arrive.

How can you protect yourself ? The most important move is to shred any loan checks before tossing them out. That's because thieves go through trash bins - it's called "dumpster diving" - to look for blank checks as well as credit card applications and other documents. If you have doubts about the security of your incoming mail, consider renting a P.O. box or making some other arrangement.

By law, you owe nothing if a thief uses a loan check made out to you. The costs fall directly on the creditors and on the companies that cash forged checks. However, some of the costs indirectly are passed on to consumers in the form of higher interest rates on loans and higher costs for merchandise. Also, you'll probably spend time and effort proving your innocence - a hassle that consumer groups say innocent victims shouldn't have to go through over a financial product they didn't ask for in the first place.

Lenders say their anti-fraud procedures are good, and getting better. They also point out that, by law, consumers can call one of three major credit bureaus (see the article Your Wallet: A Loser's Guide) to "opt out" of many unsolicited mailings for credit, including loan checks. Even so, the House Banking Committee recently held a hearing on congressional proposals to ban the mailing of unsolicited loan checks just as it now is illegal to mail unsolicited credit cards to consumers.

Final Thoughts

So, what should you do? Here's good basic guidance recently issued by the Better Business Bureau in Denver: Don't cash a loan check until you understand the full ramifications. Review all the terms of the loan. Contact a lending officer if you have concerns. Shop around and compare interest rates. Analyze your ability to repay the loan.

We leave you with this: If you're sure you don't want loan checks, consider having your name removed from future mailings. At the very least, shred unwanted checks before disposing of them. If anyone should benefit from loan checks, it should be you not a thief. You also can find out if a bank's deposits are federally insured by calling the FDIC's Division of Compliance and Consumer Affairs toll-free (see details in the For More Information section of this newsletter) or by consulting the Institution Directory on the FDIC's Internet home page. Be aware that some legitimate banks operate on the Internet using trade names that differ from the legal name of the institution. When in doubt, your best bet is to call the FDIC.

Before purchasing goods or services over the Internet: Try to find out if anyone you know has dealt with the merchant online and ask how it went, Kopchik says. If you don't have personal references for the merchant, consider asking for guidance from your local Better Business Bureau or Chamber of Commerce. Both the U.S. Chamber of Commerce and the American Institute of Certified Public Accountants have indicated that they have plans to "certify" merchants who do business over the Internet. Some Internet service providers vouch for merchants that operate from their sites. For example, America Online will cover your maximum loss from credit card fraud ($50 per card under federal law), provided you report the fraud promptly.

Be careful using your credit card number when buying over the Internet. Most reputable merchants who accept card payments over the Internet use a system that scrambles or "encrypts" your card number so it can't be read by outsiders. The latest version of some popular Internet browser programs (such as Netscape Navigator and Microsoft Internet Explorer) may be equipped with encryption technology. Your computer screen generally will display some sort of logo (for example, a "lock and key") showing that your message is being encrypted. The major credit card associations (VISA and MasterCard) also have announced plans to start a new system they say will safely transmit credit card numbers over the Internet and verify the authenticity of merchants.

Some merchants may encourage you to pay electronically without using your credit card number. Perhaps you'll be asked to maintain an "electronic wallet" with a company (CyberCash is one) that will pay the merchant on your behalf. In other cases, companies will enable you to pay a merchant using your credit card but without transmitting the card number over the Internet.

Finally, if you think you've been victimized by a fraud, contact the Internet Fraud Watch of the National Fraud Information Center, which forwards reports of suspected crimes to

federal and state authorities. Its toll-free number is 800-876-7060, and its Internet site is www.fraud.org. Or, you can report the suspected fraud directly to the appropriate federal or state agency (for example, the Securities and Exchange Commission if the company is a stockbroker).

Privacy on the Internet: As you spend time on the Internet, the various Web sites you visit may collect information about you, with or without your knowledge, regarding such things as the kinds of products you buy and the topics you find interesting. These Web sites may use this information internally or sell it to other firms or organizations. While these practices are not illegal, they may result in unwanted e-mail from unfamiliar companies or groups.

"Look to see if a Web site you are visiting discloses the company's policy about collecting and using the information it gathers," says the FDIC's Bonnette. "If it doesn't disclose its policy and you want to know more, follow up by calling or e-mailing the company." Among your other options: software from Internet service providers and computer stores that can block unwanted e-mail.

Final Thoughts

While the Internet has made it possible to bank, invest and shop from the comfort of your home, you still have to be cautious. After all, just because you "surf" the Internet you don't want a thief to "wipe out" your money.

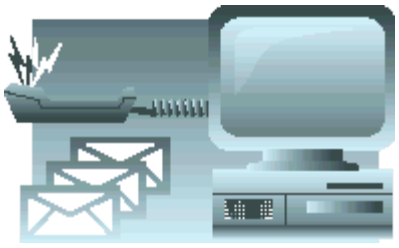
Treasury Issues Proposal to Deliver Most Federal Payments Electronically

Safety-oriented plan would eliminate paper checks, except for hardship cases

Although the Treasury proposal would require electronic payments in most cases, it would allow people facing certain "hardships" to continue receiving paper checks in the mail. As proposed, if you're a federal benefit recipient and you have an account at a financial institution, you'd be expected to sign up for direct deposit of your payments. If you don't have an account at a financial institution - and an estimated 10 million benefit recipients don't - the Treasury would open a limited-purpose account at a reasonable cost to you. However, if you have a physical disability or you face certain financial hardships or geographic barriers, you could request a waiver and continue receiving your benefit checks in the mail.

For more information about the proposal, contact the Treasury's Financial Management Service, 401 14th Street, SW, Room 420, Washington, DC 20227, phone (202) 874-6590, or read the plan on the Treasury's Internet site (www.fms.treas.gov/eft/). If you wish to express your opinions on the proposal, written comments are due to the U.S. Treasury Department by December 16, 1997. Final decisions about the costs and other features of any new accounts are expected to be announced in the spring of 1998.

More Information



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

Federal Deposit Insurance Corporation
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 information about consumer protections, including deposit insurance:

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

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

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

E-mail: consumer@fdic.gov

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

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

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

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

E-mail: ombudsman@fdic.gov

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

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 Avenue, NW
Washington, DC 20551

Phone: (202) 452-3693

Fax: (202) 728-5850

Home Page: www.federalreserve.gov

E-mail: consumer.assistance@occ.treas.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

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.

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