FDIC Consumer News

Summer 2001

Shopping and Paying From Home Over the Internet... Do Your Homework First

With the benefits come potential pitfalls, including the risk of ID theft. Here's how to protect yourself.

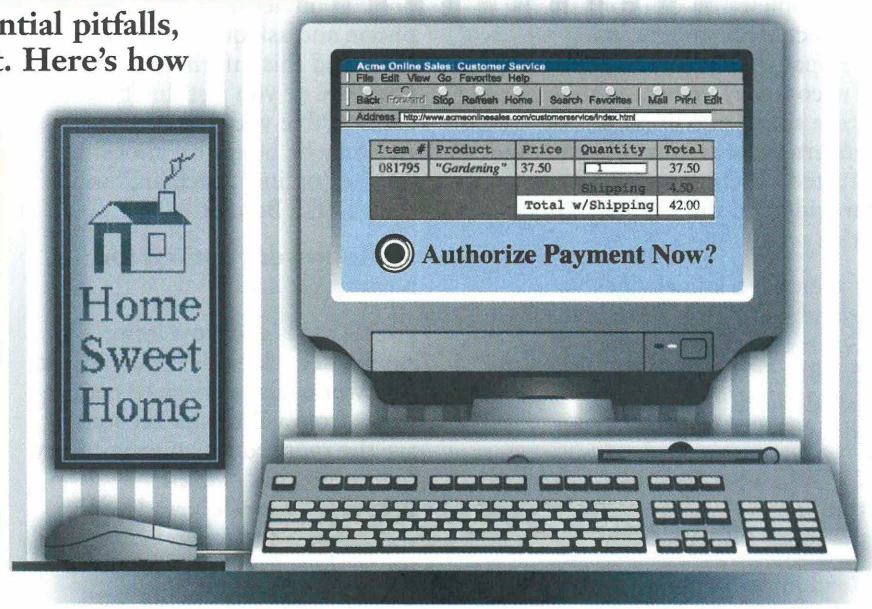


Illustration: T.W. Ballard

As people are becoming more comfortable using the Internet, they're also more willing to shop for goods and services online. After all, the Internet lets you research products, comparison shop among hundreds of businesses, sign up for special deals, and pay for your purchases 24 hours a day, seven days a week without ever leaving home. But while online shopping offers great convenience, there also can be hazards.

Perhaps the most serious risk is identity theft, which happens when criminals obtain personal information, such as a credit card or Social Security number, and use it to commit fraud in someone else's name. Much less troublesome, but still a concern, are unwanted advertisements and junk e-mail that originate when companies gather and sell information about consumers who visit their Web sites.

"Online shopping is definitely catching on," says Cynthia Bonnette, Assistant Director of the FDIC's Bank Technology Group in Washington. "But it *is* different from the way we're accustomed to shopping, and you must be careful in how you decide to share sensitive information online."

FDIC Consumer News previously published tips about safe shopping online, but given the increased popularity of Internet buying, plus new developments, such as online auctions, we are returning to the subject. Here are our simplest, best suggestions for protecting yourself:

1. Deal with a reputable company.

"Practically anyone anywhere in the world can set up a Web site anonymously," says Michael Jackson, a Senior Bank Technology Specialist with the FDIC in Washington. "That creates an environment in which parties are not always certain with whom they are doing business, and that increases the potential for fraud and other troubles." Jackson notes there have been instances of con artists and identity thieves tricking consumers into divulging credit card numbers and then buying goods or withdrawing money using the accounts of innocent victims.

How can you minimize your chances of dealing with a problem Web site?

• Stick to companies you already know from their retail outlets, mail order catalogues or other services. Be suspicious if the

continued on next page

INSIDE

Read more about Internet services beginning on Page 3

merchant doesn't list a physical address or a phone number.

• Closely review the letters and numbers in the Web site's address (URL), especially if you are provided a link to that site in an unsolicited e-mail. Some con artists try to lure consumers to their fraudulent Web sites by using corporate names or Internet addresses that are very similar to those of legitimate, well-known companies. You can confirm the correct Web address in a company's literature or by calling the company using a number from the phone book, a government agency or some other trusted source, not the one provided on the Web site (in case it's a scam).

• Contact a knowledgeable friend, your state's Attorney General's office (see Page 4) or the Better Business Bureau and ask about the merchant's reputation.

2. Take precautions to protect the privacy and security of your personal information.

Read information on the company's security practices and its privacy policy, primarily to find out how it safeguards bank account, credit card and other confidential information. For example: Does the online merchant keep personal information in its computers in an encrypted (coded) form? Is your credit card number or other personal information transmitted during an online payment also encrypted and "secure" (often indicated by a padlock logo on the computer screen)? Can you "opt out" or block certain personal information from being shared with other people or companies?

Also, provide the minimum information needed to complete a transaction. Don't divulge your Social Security number, credit card number, address, phone number or other personal information unless you're sure the Web site is legitimate and you know why that information is needed. And never disclose your password to anyone. "Don't even provide your password to customer service representatives," Jackson says. "They don't need that information to assist you."

If you don't understand something about a Web site's security procedures or privacy policy, contact the company by phone and ask questions. "If you can't find this information on the Web site or you just don't feel comfortable with the situation, you may be better off choosing another online merchant," warns the FDIC's Bonnette.

3. Know your options for paying.

Credit cards and, to a lesser extent, "check cards" (a debit card that works like a check to deduct funds from your bank account) are the most common ways to pay online because of their convenience, widespread acceptance, and federal consumer protections (see Page 4). Remember: Protect your card numbers by shopping at Web sites that encrypt your card number so they can't be read by outsiders. Also look into new security methods (such as temporary, substitute account numbers) that let you use your credit card without providing your *real* account number or password online.

Bonnette also notes there are other ways to pay merchants electronically. Examples include:

• "Electronic cash," also called "digital cash," which is a form of electronic currency that can be purchased, downloaded and stored on the hard drive of your computer or a special card;

• Deductions from pre-arranged accounts with online payment services (see the article about e-mailing money on the next page);

• Additions to your monthly phone bill or other utility bills;

• Bonus points you earn that can be used to make additional online purchases from participating merchants; and

• "Electronic checks," which generally involve sending instructions to have the funds deducted electronically from your checking account.

If you're unsure about the pros, cons and consumer protections for a particular way to pay, Bonnette suggests that you ask about such things as the security procedures and how quickly funds will be sent or received.

4. Be prepared for a possible problem.

Before you make a purchase or a payment, read the information on the Web site regarding your right to stop payment or the company's refund and return policies for damaged goods or faulty service. Print out copies of purchase orders and confirmation numbers in case there's a dispute. Also regularly check your bank and credit card account statement for errors or unauthorized withdrawals.

Remember that, depending on the situation, you may be protected by federal and state laws against such woes as account errors, unauthorized use of your account information, and the unwanted sharing or selling of your personal information. Several major federal laws are cited in the box on Page 4. And if you need help understanding your rights or resolving a problem, a federal or state government agency (also on Page 4) may be able to assist you.

The bottom line about shopping and paying online from home—it *can* be safe and easy, but you've got to do your homework before entrusting your personal and financial information to just any Web site.

Now Arriving By E-Mail... Money

But consumers should consider potential risks

If you've got an e-mail address, you've now also got the capability to get money to or from other people online. It's called a person-to-person payment, or "P2P" in the language of electronic commerce. These systems are commonly used to pay for items at online auctions or to send money to friends and family members far away. But while this relatively new Internet option offers convenience, "consumers also should think about the potential risks," says Michael Jackson, an FDIC Senior Bank Technology Specialist.

In general, P2P works like this: If you'll be sending money, you must open an account with a service provider, which may be a bank or an Internet company. You'll be asked to provide key pieces of information, such as bank or credit card account numbers, and in some cases maybe even your Social Security number. To send a payment, you'll fill out an online form that asks for the dollar amount and the recipient's e-mail address. The payment likely will be charged to your credit card or deducted from your bank account. If you're receiving the payment, you'll get an e-mail about the payment along with instructions for getting the funds via a check in the mail, a credit to your bank or credit card account, or a direct deposit into an account at the P2P service provider for your own use in sending e-mail payments.

What are the potential risks? According to the FDIC's Jackson, there have been instances of fraud and identity theft, erroneous or unauthorized withdrawals from accounts, and failure to deliver the promised goods. (Note: The Federal Trade Commission says problems with Internet auctions are the #1 complaint of online consumers, who report paying for items that were misrepresented or that didn't arrive at all.)

To minimize risk, follow the basic suggestions in our cover story. For example: Deal only with a reputable company. Read the privacy and security policies posted on the Web site. Understand how the service provider or government regulations will protect you from unauthorized withdrawals and other troubles.

And, be aware that not all of the companies offering this service are banks. "This doesn't mean that nonbanks are unsafe to use," Jackson says, "but that, in some situations, where you can go for help and the procedures for handling consumer complaints may differ from those for banks."

If you're likely to have a significant amount of money in an account provided by an online service provider, also read the Web site's "terms of use" or ask a customer service representative to find out whether the funds are protected against loss. Keep in mind that only funds placed in a deposit account at an insured bank or savings association are protected by FDIC insurance.

Read FDIC Tips for Banking Over the Internet

To read or print the FDIC brochure "Tips for Safe Banking Over the Internet," go to www.fdic.gov/bank/individual/online/safe.html on the FDIC's Web site. Or, order single copies from the FDIC's Public Information Center listed at right.

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, *Writer-Editor*

Tommy Ballard, *Graphic Design & Illustration*

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

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

Subscriptions

Subscriptions are available free of charge. Send subscription requests or address changes to: FDIC Public Information Center, 801 17th Street, NW, Room100, Washington, DC 20434
Phone: (800) 276-6003 or (202) 416-6940
E-mail: publicinfo@fdic.gov
Fax: (202) 416-2076

On the Internet

Consumer information from the FDIC is available at www.fdic.gov.

Find current and past issues of ***FDIC Consumer News*** at www.fdic.gov/consumers/consumer/news/. 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.

Before You Aggregate... Investigate!

Another new Internet service called account aggregation enables you to organize and monitor information about practically all of your assets—your bank accounts, credit cards, investments, insurance policies, even your frequent flyer miles—using just one Web site and one password. Before you aggregate, Cynthia Bonnette, Assistant Director of the FDIC's Bank Technology Group, suggests:

• **Check out the company.** "To enroll with an aggregation service you have to provide your account numbers and passwords," Bonnette says. "Think carefully before providing this information to anyone because their practices for securing and sharing your information are very important." For guidance, see our cover story.

• **Review the policies, terms and conditions of the service.** Read about the company's privacy and security policies, so you understand how your information will be protected. Also note the company's procedures for accepting customer complaints and resolving problems.

• **Determine how timely and accurate the information will be.** Not knowing whether the information is outdated or erroneous could cause you to make a bad or costly decision.

• **Contact the institutions that hold your accounts.** Make sure it's OK to disclose your password and other information to an aggregation service.

Bonnette adds that account aggregation services in the future could become more common and more interactive, perhaps including the capability to conduct financial transactions or receive personal financial advice online.

Federal Laws That Can Help

The Electronic Fund Transfer Act (EFTA) protects you against accounting errors and unauthorized withdrawals involving debit card transactions (deducted directly from your bank account) by personal computer, ATM or other electronic device, if you report the problem promptly. Perhaps the biggest protection for online shoppers is the right to correct errors or unauthorized charges if you contact your financial institution within 60 days after the statement containing the problem was sent. Also, in cases of lost or stolen cards, "the EFTA limits your liability for unauthorized transfers to a maximum of $50 if you notify the bank within two days after discovering the loss or theft," explains FDIC attorney Robert Patrick. Eric Kooistra of the FDIC's Division of Compliance and Consumer Affairs notes that in many situations the major bank cards will voluntarily cover all losses from unauthorized transfers "as a way to promote worry-free use of your credit card and debit card online."

The Fair Credit Billing Act, part of the Truth in Lending Act, generally protects consumers from unauthorized transfers, billing errors and other liability when they make an online payment using a credit card. This law also may allow you to withhold payment on defective goods or services purchased with a credit card.

The Gramm-Leach-Bliley Act of 1999 gives you the limited right to "opt out" or stop your financial institutions from sharing personal information with non-affiliated third parties. Rules from the FDIC and other federal regulators say that if you use your credit card or debit card to conduct transactions online, the personal information collected in the process is subject to the opt-out provisions of the law. A financial services company that does business on the Internet also is required to clearly state its privacy policy. (See next page.)

Note: Consumer protections also may exist in state laws.

Government Agencies That Can Help

Federal banking regulators (listed on Page 7) enforce consumer protection laws involving transactions with the federally insured banks, savings associations or credit unions they supervise.

The Federal Trade Commission enforces consumer laws involving nondepository institutions. Write to the FTC's Consumer Response Center, 600 Pennsylvania Avenue, NW, Room 130, Washington, DC 20580, call toll-free 877-FTC-HELP (877-382-4357), or go to www.ftc.gov. The Web site also includes consumer brochures about safe shopping online, identity theft and Internet frauds to avoid.

Your state government or the state government where the company is located may have the authority to assist consumers in matters involving alleged fraud or unfair or deceptive practices. Start with the state's Attorney General's office, which you can locate in the government (blue) pages in your local phone book or from the National Association of Attorneys General at www.naag.org/about/aglist.cfm.

The Internet Fraud Complaint Center, a joint effort of the FBI and the National White Collar Crime Center, accepts consumer complaints about possible Internet scams. For more information, go to its www.ifccfbi.gov Web site.

The Latest on Your New Rights to Privacy... Our Answers to Your Questions

In the Winter edition of ***FDIC Consumer News***, we described your new rights to financial privacy under the Gramm-Leach-Bliley Act of 1999. This federal law requires your financial institutions to provide notices describing the type of information they intend to share with third parties and how customers may "opt out" or say "no" to information sharing under certain circumstances. Financial institutions were required to send these notices to existing customers by July 1, 2001. New customers also will get privacy notices, and all customers will receive a notice annually. We previously invited readers to submit questions about their financial privacy rights. Here are some of the questions we received, and our answers.

Can I contact my bank and credit card companies to request that they not share my information or do I need to fill out a form?

Financial institutions that intend to share non-public personal information about consumers with other companies must give those individuals a chance to opt out, with certain exceptions (such as for information needed to process loans, mail account statements or conduct other normal business). But when it comes to *how* customers can opt out, the rules leave that up to each financial institution, provided the procedures are reasonable.

Institutions described their opt-out procedures in the mailings required by July 1 of this year. For example, your institution may require you to complete and return a form, or it may require you to call a certain phone number. "To ensure that your request is honored, it's important to follow the institution's opt-out instructions," says Ken Baebel, Assistant Director of the FDIC's Division of Compliance and Consumer Affairs. If you don't have a copy of your institution's requirements, call the customer service department and ask how to opt out.

Some of the institutions don't say anything about contacting them to opt out, yet according to the notices, these institutions are sharing plenty of information. When can an institution share information without giving a customer a chance to opt out?

Under the Gramm-Leach-Bliley Act, you cannot stop an institution from providing personal information to *outside* companies and organizations if, for example, the information is used to:

- Market the institution's own products or services;
- Market certain products or services jointly with another financial institution.
- Enable a third party to help conduct normal business for your institution, such as handling data processing for accounts or mailing account statements.

In addition, the federal Fair Credit Reporting Act (FCRA) allows an institution to share with affiliates (other parts of the *same* corporate family) certain information based on your transactions with the institution. This kind of information sharing also can be done without giving you an opportunity to say no.

Example: Your bank can tell an affiliated brokerage firm that you have a certificate of deposit about to mature, so it can offer you an investment alternative. Your bank, however, cannot provide an affiliate with personal information from, say, your credit report or loan application unless you're given a chance to opt out first (because that information is *not* based solely on transactions you've conducted with the bank).

If I send the proper notice that I wish to opt out, do I have to redo this form each year or will my initial notice remain in effect?

You do not need to renew your opt-out instructions with a bank or other financial institution. One request will remain in effect indefinitely unless you contact the institution asking to cancel it. But let's say your institution later decides to expand how much

continued on next page

Any Other Questions About Financial Privacy?

Write to: ***FDIC Consumer News***, 550 17th Street, NW, Washington, DC 20429. You also can send an e-mail to jrosenstein@fdic.gov or fax your questions to 202-898-3870. Please include your name, address and phone number. No names will appear in print without permission.

customer information it intends to provide to other companies. If it's the kind of information the law says you have a right to prevent from being shared, "your institution must provide you with a revised privacy notice and give you an opportunity to opt out of the new information sharing," says Deanna Caldwell, a Senior Policy Analyst for the FDIC's Division of Compliance and Consumer Affairs. "This is another example why we say you should pay attention to every privacy notice you get from your financial institutions."

We've also been asked what happens to a consumer's opt-out request if your bank merges with another institution and the "new" bank has a privacy policy that is *less* protective of your personal information. Here, the merged institution must give you the right to opt out before it could apply that less-protective policy to your personal information.

If I opt out of information sharing because I don't want unsolicited offers, does this prevent my bank from reporting my creditworthiness to credit bureaus and, therefore, to other institutions I may be applying to for credit?

No, even if you opt out, your bank or other financial services firms still can, and will, report private information to credit bureaus. Why? Because the privacy law specifically permits institutions to provide nonpublic personal information to credit bureaus.

Credit bureaus are companies that collect facts about a person's financial responsibility, such as the timeliness of loan payments. Banks rely on reports from credit bureaus when deciding, for example, to grant a loan or a credit card to a particular consumer, and those reports can only be prepared if financial institutions maintain a regular, free flow of information to credit bureaus.

Friends and relatives have forwarded to me the same anonymous e-mail message warning that, as of July 1, 2001, credit bureaus can share my credit information, mailing address, telephone number and other information "to anyone who requests it" unless I opt out. Is this true?

No, that's a false rumor being widely circulated on the Internet. It's apparently based on someone's misinterpretation of the July 1 date in the Gramm-Leach-Bliley Act for banks and other financial institutions to send out privacy mailings to customers. Here's what you should know: Credit bureaus can't release the information in your credit report to just anyone who asks for it. Under the Fair Credit Reporting Act, a credit bureau can only provide this information to people and businesses with a legitimate right to obtain it, as specified in the law. For example, a company has a right to get your credit report if you apply for a credit card, a home equity loan or an insurance product.

However, there *are* opt-out provisions in the FCRA. One, for example, gives you the right to prohibit credit bureaus from providing information to companies that want to send you unsolicited offers of credit or insurance. The easiest way to remove your name from these special marketing lists sold by credit bureaus is to make one toll-free phone call to 888-5-OPTOUT (888-567-8688), a service operated on behalf of the nation's largest credit bureaus. A phone request to the credit bureaus is only good for two years. Thereafter, you would have to call again to renew for another two years. To opt out indefinitely, you must submit a written request using a special form that you can order from the toll-free number.

The central phone service for credit bureau opt-outs is an automated system that will ask you to leave personal information, including your Social Security number. While this automated service promises confidentiality, if you are reluctant to leave your Social Security number, then you should write a letter (not an e-mail) to any one of the credit bureaus listed below and ask it to share your opt-out request with the other companies. Be sure to include your full name, address, Social Security number and signature. Also specify if you want to opt out for two years or indefinitely, in which case you will receive the form to complete. Write to:

• Equifax Inc., Options, P.O. Box 740123, Atlanta, GA 30374-0123;

• Experian, Opt-Out, P. O. Box 919, Allen, TX 75013-0919;

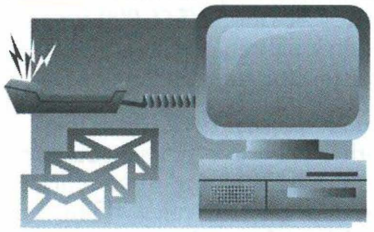
• Innovis, Consumer Opt Out, P. O. Box 219297, Houston, TX 77218-9297; or

• TransUnion, Name Removal Option, P.O. Box 97328, Jackson, MS 39288-7328.

For More Information About Your Privacy Rights

Contact your financial institution or one of the federal regulatory agencies listed on the next page for more details about your rights to financial privacy. Also take a look at our story about the new privacy protections in the Winter 2000/2001 edition of ***FDIC Consumer News***. Find it on the Web at www.fdic.gov/consumers/consumer/news/cnwin0001 or contact the FDIC's Public Information Center (Page 3) to request a single copy.

For 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 insures deposits up to $100,000 at federally insured banks and savings associations. For more information, contact the FDIC's Division of Compliance and Consumer Affairs. The National Credit Union Administration insures deposits up to $100,000 at federally insured credit unions. Addresses and phone numbers are listed on this page.

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

Toll-free Phone: **(877) ASK-FDIC** or **(877) 275-3342**
TTY: **(800) 925-4618**
8:00 a.m. to 8:00 p.m. Eastern Time

Home Page: **www.fdic.gov**

For written inquiries about deposit insurance or consumer protection laws, or to submit a complaint about an FDIC-supervised institution:

FDIC Division of Compliance and Consumer Affairs

Mail: **See address at left**

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

E-Mail: Use our Customer Assistance Form on the Internet at **www2.fdic.gov/starsmail/index.html**

For written inquiries involving problems or complaints related to the FDIC:

FDIC Office of the Ombudsman

Mail: **See address at left**

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

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**

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

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

Division of Consumer and Community Affairs
20th Street and Constitution Ave., NW
Washington, DC 20551

Phone: **(202) 452-3693**

Fax: **(202) 728-5850**

Home Page: **www.federalreserve.gov**

National Credit Union Administration
Charters and supervises federal credit unions. Insures deposits at federal credit unions and many state credit unions.

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

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

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

Home Page: **www.ncua.gov**

E-mail: **pacamail@ncua.gov**

Office of Thrift Supervision
Supervises federally and state-chartered savings associations plus federally chartered savings banks. (The names often identify them as savings and loan associations, savings associations or savings banks. Most federally chartered savings associations have the word "Federal" or the initials "FSB" or "FA" in their names.)

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

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

Home Page: **www.ots.treas.gov**

E-mail: **consumer.complaint@ots.treas.gov**

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

New Tax Law Enhances Savings Programs for Retirement, Education

The tax cut signed into law by President Bush on June 7, 2001, includes provisions that are of significant interest to financial institution customers, including new incentives for Americans to save for retirement and education. Here are some highlights.

Retirement Savings: Contribution limits for Individual Retirement Accounts (IRAs), including those for Roth IRAs (which differ from regular IRAs primarily because the earnings may be tax-free), will gradually rise from the current $2,000 a year to $5,000 a year by 2008. Contribution limits also are increasing for employer-sponsored retirement plans, such as 401(k) accounts. For example, the new law gradually raises the maximum annual contribution to 401(k) accounts from the current $10,500 to $15,000 in 2006. Also, taxpayers at least 50 years old can make extra payments into IRAs, 401(k)s and other retirement accounts, depending on the plan, up to an additional $1,000 in 2002, and eventually up to $5,000 in 2006.

Education Saving: Earnings on Education IRAs, which are accounts established to pay for a child or another beneficiary to attend school, generally are exempt from federal taxes if they don't exceed the student's education expenses. Under the new law, the maximum contribution will increase from the current $500 to $2,000 per year starting next year, and distributions are tax-free, not just tax-deferred. For the first time, employers will be permitted to contribute to an employee's Education IRA, up to the statutory maximum dollar amount. In addition, the proceeds from an Education IRA also will become available to pay for elementary and secondary school tuition, no longer only for the costs of higher education.

Student Loans: Currently, you can deduct up to $2,500 of interest expenses on student loans. Starting in 2002, there will be no limit on the amount you can deduct if your income is below set levels ($55,000 for an individual return and $100,000 for joint filers).

In an unusual twist, these and other tax breaks are scheduled to expire in 2011 and to be replaced by the "old" tax rules. "This quirk in the tax law may add some uncertainty to your long-term tax planning, but even so, there are still significant benefits you can take advantage of for at least the next several years," says Rick Cywinski, an FDIC tax policy manager in Washington. "And while there's no guarantee, it's very possible that between now and 2011 Congress will extend or even enhance these new tax-savings provisions."

Cywinski and other FDIC officials suggest that you consult with your tax preparer, financial planner or another trusted advisor if you have questions about the tax law or what it could mean for your finances.

FDIC
Federal Deposit Insurance Corporation
Washington, DC 20429-9990