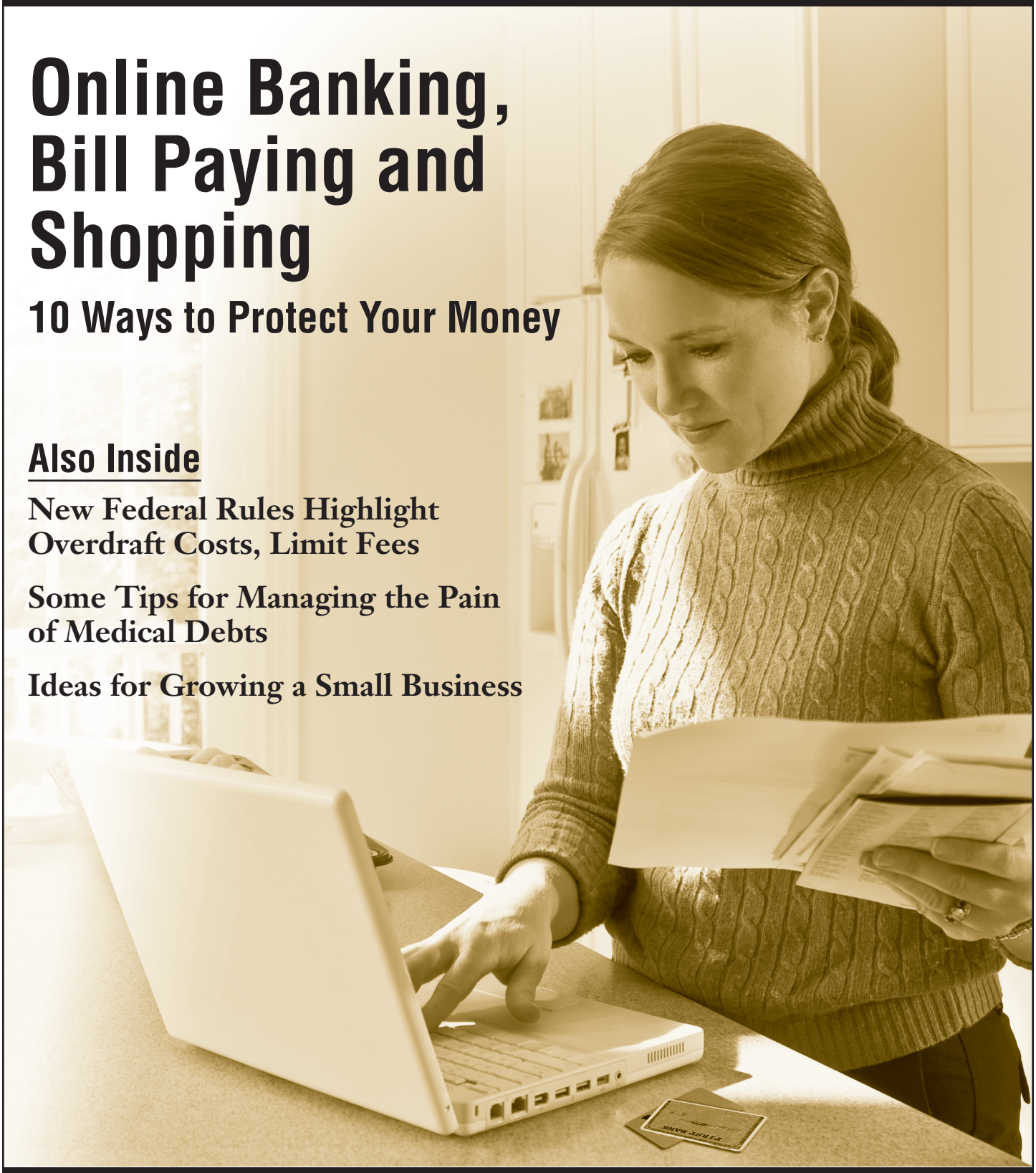
FDIC Consumer News
Winter 2009/2010

Online Banking, Bill Paying and Shopping

10 Ways to Protect Your Money



Also Inside

New Federal Rules Highlight Overdraft Costs, Limit Fees

Some Tips for Managing the Pain of Medical Debts

Ideas for Growing a Small Business

FEDERAL DEPOSIT INSURANCE CORPORATION

Online Banking, Bill Paying and Shopping: 10 Ways to Protect Your Money

Internet commerce is fast and convenient, but as with the old-fashioned ways of doing business, it pays to take precautions

Online banking, bill paying and shopping are conveniences that most people want to enjoy. And most of the time, high-tech transactions are completed quickly and without a glitch. However, just as with other transactions, in a small percentage of cases something goes wrong. That's why you need to take precautions against theft and errors.

In particular, even as banks and merchants tighten up security, Internet thieves devise new, sophisticated ways to trick consumers into sending money or into revealing information that can be used to commit fraud. "Today's Internet threats wear many different disguises, from fake Web sites to fraudulent text messages on cell phones," warned Michael Benardo, Chief of the FDIC's Cyber-Fraud and Financial Crimes Section. "That's why online consumers need to be aware that they may be targeted and they should always be on guard."

David Nelson, an FDIC fraud specialist, added: "Online fraud is an ongoing game of cat and mouse. Crooks continuously hunt for security holes, banks and merchants plug those holes, and then the criminals find new ones to slink through. But consumers play an important role in keeping crooks at bay by being aware of the potential risks, taking precautions and remaining vigilant."

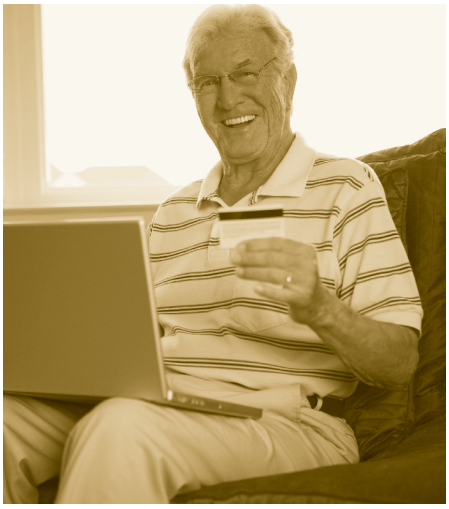
FDIC Consumer News, which periodically issues guidance to consumers regarding online precautions they can take, offers our latest collection of top tips. Note: Not all financial institutions offer each product or service described here.

1. If you bank online, frequently check your deposit accounts and lines of credit to spot and report errors or fraudulent transactions, just as you should with traditional banking. "Your ability to monitor your accounts online has gotten easier, faster and more convenient now that banking by cell phone is starting to mature alongside banking online," said Michael Jackson, Associate Director of the FDIC's Technology Supervision Branch. "This is important, because the sooner you can detect a problem with a transaction, the easier it should be to fix."

Nelson suggested checking your accounts online about once or twice a week, but he also noted that "more and more banks are making it easier for their customers to keep an eye on their accounts electronically. For example, many banks offer e-mail or text message alerts when your balance falls below a certain level or when there is a transaction over a certain amount."

Federal laws generally limit your liability for unauthorized electronic funds transfers, especially if you report the problem to your financial institution within specified time periods, which will vary depending on the circumstances. A good rule of thumb is to check your statements promptly and report unauthorized transactions to your bank as soon as possible.

2. Never give your Social Security number, credit or debit card numbers, personal identification numbers (PINs) or any other confidential information in response to an unsolicited e-mail, text message or phone call, no matter who the source supposedly is. Chances are an "urgent" e-mail or phone call appearing to be from a government agency (such as the IRS or the FDIC), a bank, merchant or other well-known organization may be a scam attempting to trick consumers into divulging personal and account



information. It's called "phishing," a high-tech variation of the concept of "fishing" for personal information.

Also watch out for phishing scams that involve bogus text messages sent to cell phones claiming that a bank account has been "blocked" and the recipient must call a certain number to fix the problem. If you make that call, you likely will be asked to enter your account number and PIN. The criminals can use this information to make counterfeit debit cards and drain your account.

"Real bankers and government officials don't contact people asking for this kind of information," said Benardo. "Your bank will already have your account numbers and only you should know your log-in credentials, and a government agency won't have a need for this information."

3. Don't open attachments or click on links in unsolicited e-mails from anyone you don't know or you otherwise aren't sure about. Sometimes these attachments or links can infect your computer with "spyware" that can change your security settings and record your keystrokes. "Spyware can secretly steal your passwords, bank or credit card numbers, and your answers to security questions like your mother's maiden name or your high school," Benardo advised. "Online thieves can use this information to log into your account, make changes and transfer money, leaving your bank account empty."

In one recent example, criminals sent out fake IRS e-mails warning recipients that they were being investigated for unreported income and asking them to click on an attachment for more information. The file launched a program that allowed hackers to install spyware and other unwanted programs on personal computers (PCs) to access bank accounts.

4. Watch out for sudden pop-up windows asking for personal information or warning of a virus. This is called "scareware" because it frightens people into providing information, downloading malicious software or paying for removal. If you get an e-mail or pop-up window saying your computer has a virus and it offers a program to clean your PC — and the warning window won't go away — your first step is to use the computer's "task manager" function and click "end task" or "force quit" to shut down the pop-up window. Scareware can be a nuisance to clean off your computer, so call your anti-virus software company if you need help.

5. Use a mix of security tools and procedures. "Staying safe online is like protecting your home with lighting, locks, alarms and fire extinguishers," explained Nelson. "You can't rely on just one layer of defense to protect you from all online threats."

At the top of the list of security tools to use — and keep updated — are anti-virus software to detect and block spyware and other malicious attacks, and a "firewall" to stop hackers from accessing your computer.

Even if your computer seems fine, Nelson said, schedule an automatic anti-virus scan to run at least once a week but preferably every day. Call or e-mail your anti-virus vendor right away if you get a warning message and you don't know what to do next.

Also consider these extra precautions as you use the Internet:

• *Don't log into your bank account while using public computers, such as at a library, or free wireless connections at coffee shops and similar places.* Criminals often try to intercept Internet traffic, including passwords, from these locations.

• *Pay attention to the toolbars at the top of your screen.* Current versions of the most popular Internet browsers and search engines often will indicate if you are visiting a suspicious Web site.

• *Choose "strong" user IDs and passwords that will be easy for you to remember but hard for hackers to guess.* The strongest ones have a combination of letters, numbers and other characters, and are at least 10 characters long. For your online banking, choose IDs and passwords that are not the same as those you use for e-mails or social networking sites, just in case they get into the wrong hands. Also change your online banking password about every 90 days. And if you remove a computer virus from your PC, immediately change your password.

• *Have each person in your household bank and shop online and send e-mail through his or her own "standard user account."* Not conducting these online activities through the computer's "administrator account" — the one that makes changes affecting all users — reduces the likelihood that a hacker can install unwanted programs on your PC. Limit the use of the administrator account to special tasks needed for your computer, such as adding or removing software and installing updates to your operating system.

• *Consider using a separate computer solely for online banking or shopping.* A growing number of people are purchasing basic PCs and using them only for banking online and not Web browsing, e-mailing, social networking, playing games or other activities that increase the chances of downloading malicious software. You can also consider using an old PC for this limited purpose, but you should uninstall any software you no longer need and follow up with a scan of the entire PC to check for malicious software.

• *Only use security products from reputable companies.* Nelson said one way to check out these products is by reading

continued on next page

Depositing Paper Checks Over the Internet

New technology turns your scanner or cell phone into a bank teller

Don't feel like walking or driving to your bank to deposit a check? Rather not spend the time and the money to mail it in? You may have a relatively new option — the ability to "deposit" paper checks electronically over the Internet. What you need is a scanner (to capture an image of the check) and a personal computer (to securely transmit the image online), or a cell phone equipped with a digital camera that can do similar duty. And, of course, your bank must offer the service, which has become much more common in just the last year.

Known in the banking and technology industries as "remote deposit capture"or RDC, this service is mostly marketed to small businesses that typically are paid by check and want to be able to quickly deposit those payments. However, consumers also can benefit, especially if they receive a lot of checks and find it inconvenient to go to their local branch or ATM.

"RDC can save consumers time and money because you don't have to bring or mail your checks to deposit them," said Jeff Kopchik, an FDIC Senior Policy Analyst specializing in technology matters. "In addition, RDC allows you quicker access to the funds because checks deposited over the Internet are generally available in one or two business days as opposed to five business days for regular paper checks."

And if you use RDC, Kopchik added, ask your bank how to properly transmit the check images and how to safeguard your equipment and the original paper checks.

reviews from computer and consumer publications. "Look for a product that has high ratings for detecting problems and for providing tech support if your computer becomes infected," he said.

Kathryn Weatherby, a fraud specialist at the FDIC, also cautioned that banks normally don't ask their customers to download software updates. "If you get an unsolicited request to update your banking software," she said, "independently verify it by calling your bank using a phone number from your bank statement, not the phone number that appears in the request, which could connect you to a scam operation instead of your bank."

6. Beware of check scams. With unemployment high, con artists are preying on people who need cash. One common check scam involves attractive offers — usually originating in e-mails or online job postings — involving part-time work from home. As the new "employee," you will be sent a check to deposit (which will be counterfeit) and told to forward cash from your own account (to the crooks). Another scam involves "mystery shopper" programs where the new hire is given fake money orders or checks and asked to wire funds to the criminals. And unlike electronic transfers that are covered by consumer protection laws, fraudulent check scams often leave consumers suffering the loss.

7. When shopping online, deal with reputable merchants and be wary of unbelievably low prices. "There is no guaranteed way to ensure that an online merchant you're unfamiliar with is reputable, but there are ways to avoid doing business with an unreliable one," cautioned Jeff Kopchik, an FDIC Senior Policy Analyst specializing in technology matters.

First, he said, ask your friends and family if they've had good experiences with a merchant you're considering using. "If people you know have used and can recommend an online merchant, that's a strong indicator," he added. Second, you may already know and like some online merchants from their retail outlets, mail order catalogues or other services. They are likely to be a safer bet than an unfamiliar merchant that doesn't list a physical address or a phone number on its Web site.

If you are uncertain about an online merchant, check with the Better Business Bureau Online (www.bbbonline.com). You can also search online for complaints about the business. Similarly, if you have a problem with an online merchant, file a report with the Better Business Bureau. The Bureau will notify the merchant about your concern and ask you if the issue was resolved. A legitimate merchant will attempt to fix the problem, while a crooked company may have many unresolved issues.

8. Using a credit card generally offers more purchase protection than a debit card or other electronic forms of online payment. "Unlike paying with a debit card and the money being immediately transferred out of your account, with a credit card you generally have weeks to pay your bill," Kopchik said. "So if the merchant does not deliver as promised, you have time to dispute the transaction and even enlist the help of your credit card company." He also noted that federal law gives you certain rights, in areas such as dispute resolution, when buying with a credit card.

However, watch your budget when using your credit card to shop online. Kopchik said studies have shown that people spend more when they use a credit card instead of cash, a gift card or a debit card.

9. Be on guard against scams hiding behind online coupon offers. Web sites for legitimate coupons will only ask consumers to provide an e-mail address in order to use their service to search for online specials and discounts. Beware of any coupon site that asks for personal, financial or payment information, which can be misused by criminals.

10. Be careful if you download banking software onto a cell phone. Many cell phones called "smart phones" allow consumers to add computer-like features ranging from video games to "mobile" banking. But cell phone users need to be aware of an emerging threat from criminals selling malicious software for mobile banking, some even falsely displaying bank logos. "These applications may contain spyware, and downloading them could be giving a hacker access to your bank account or payment card information," reported Nelson.

His advice? "Only download mobile banking applications from a safe site, such as your wireless provider, phone manufacturer or your bank." When in doubt, he added, "contact your bank before downloading any banking applications to your cell phone."

For More About Internet Commerce

The Federal Deposit Insurance Corporation has consumer brochures and articles in ***FDIC Consumer News*** about banking and paying online, plus a multimedia presentation on identity theft called "Don't Be an Online Victim." Start at www.fdic.gov/quicklinks/consumers.html or call toll-free 1-877-275-3342.

Other federal financial banking agencies also respond to consumer inquiries and produce educational material on Internet banking, bill paying and shopping. Visit www.mymoney.gov and search by topic.

The Federal Trade Commission Web site at www.ftc.gov/bcp/menus/consumer/tech.shtm has good information on how to use the Internet safely, especially the "OnGuard Online" site. You can also call toll-free 1-877-382-4357.

Financial institutions, Internet service providers, consumer organizations and the news media publish tips and information you can find by searching the Web. Also contact your bank if you have a question or concern about banking or paying online.

New Federal Rules Highlight Overdraft Costs, Limit Fees

If you write a check or use your ATM or debit card when you don't have enough funds in your account, your bank may cover the transaction — but typically for a sizeable fee. Now here's good news. Changes in federal regulations will require institutions to more clearly inform consumers about the costs of overdraft services.

"An overdraft should be an infrequent or occasional event, but many of today's automated overdraft programs make it possible to incur several in a single day and rack up related fees quickly," said Luke Brown, the FDIC's Associate Director for policy involving bank compliance with consumer regulations. "The new regulations are a step toward helping consumers understand the costs of overdraft programs and assisting them with making more informed choices about the best product for covering occasional overdrafts."

Under the first new rule from the Federal Reserve Board, effective January 1, 2010, all financial institutions must clearly tell consumers on their periodic statements how much they have been charged in overdraft fees during the statement period and for the calendar year to date. This rule can help people monitor how the fees they have paid add up. It also can serve as an incentive to prevent overdrafts.

In addition, when an institution provides a consumer with account balance information through an automated system — including an ATM, Web site or telephone — it must provide the actual balance, *without* additional amounts that could be used to cover overdrafts. However, an institution may disclose a second balance that *does* include overdraft coverage, but only if the additional amount is clearly labeled (for example, by stating that the balance includes "overdraft funds").

"We hope these changes will help consumers understand how much money they actually have in their accounts, and that extra costs are associated with withdrawing more than that amount," added Sam Frumkin, an FDIC Senior Policy Analyst.

And, under another new rule from the Federal Reserve Board, beginning on July 1, 2010, financial institutions will be prohibited from charging fees for overdrafts on ATM withdrawals and one-time debit card transactions at "point of sale" (POS) terminals in stores unless the individual agrees up front ("opts in") to pay those fees. First, though, consumers must have been provided a notice explaining the institution's overdraft payment services, including the relevant fees. This information will help consumers weigh the pros and cons of various options before deciding whether or not to enroll. You can also change your mind and opt out even after you sign up.

That same rule also will prohibit financial institutions from discriminating against consumers who don't opt in for overdraft services for ATM and POS transactions by offering them accounts with less attractive terms, features and pricing.

FDIC officials also encourage consumers to become knowledgeable about alternatives to high-cost overdrafts programs.

"Consumers would benefit from information about all of the overdraft payment services or products offered by their bank, including comparative details about fees and costs," explained Mira Marshall, an FDIC Section Chief specializing in consumer issues. "Available alternatives to high-cost products could include linking a checking account to a savings account, obtaining an overdraft line of credit, and getting a small-dollar loan that may be less expensive than an overdraft program."

If you're concerned about running short on funds in your account, ask your bank ahead of time about options that may be less expensive than an overdraft program.

And regardless of whether you enroll in an overdraft program, Luke W. Reynolds, Chief of the FDIC's Community Outreach Section offered this advice: "Keep track of your account balance and make sure you have enough money in your account to cover transactions, so you avoid costly fees and embarrassment by spending more money than you have available."

News Briefs

Reminder: Key Protections for Credit Card Users Taking Effect

As reported in our Summer 2009 issue, major new protections for credit card users took effect on February 22, 2010, in areas such as prohibitions and restrictions on rate increases, limits on fees and interest charges, and improved disclosures. For more information, including changes that took effect on August 20, 2009, and more coming August 22, 2010, see our article at www.fdic.gov/consumers/consumer/news/cnsum09/newlaw.html. Also, the Federal Reserve Board has summarized key provisions for consumers at www.federalreserve.gov/consumerinfo/wyntk/creditcardrules.htm.

Beware of False Representations of FDIC-Owned Real Estate Sales

The FDIC is warning the public that individuals and companies are falsely claiming to represent the agency in the sales of properties acquired from failed institutions and are charging a fee for services available free from the FDIC. Visit www2.fdic.gov/drrore for free information about FDIC-owned properties for sale, the management companies working with the FDIC, and local brokers.

Some Tips for Managing the Pain of Medical Debts

Think twice before using your credit cards, home equity or retirement savings

With healthcare costs soaring and family budgets tightening, it's no wonder that medical debts are a major headache for many Americans. If you're facing the financial and emotional stress of medical bills and you're not sure how — or if — you can pay them, here are some suggestions from ***FDIC Consumer News***.

Guard against billing and insurance errors. Get an itemized statement from each health care provider and make sure the services and costs listed are correct. Contact your provider if you find a mistake or you need clarification. Also, if you believe your health insurer denied or reduced a payment incorrectly, you may appeal that decision with your insurer. Check also with your state's department of insurance for any other rights you may have.

Contact the doctor's office or hospital immediately if you don't think you can pay a medical debt. Explain your situation and try to negotiate the bill or offer a reasonable payment plan before it is referred to a collection agency. "Medical debts that go unpaid can be reported to the credit bureaus and damage your credit record," said Bobbie Gray, an FDIC Community Affairs Specialist. "Not only will you still have debts, but you may end up paying more to borrow money in the future, if you're approved to borrow at all."

For big medical expenses that are not covered by insurance, think twice before charging them to a credit card or a loan with a high interest rate. If you expect to pay the bill back over a long time period — perhaps over several years — the interest costs can end up far exceeding the charges from your healthcare providers. Also, putting a medical bill on your credit card results in the expense no longer being considered a medical debt, and that may limit the ability of low-income patients to obtain financial assistance from Medicaid or other programs. Instead of turning to credit cards for medical bills you're sure you can't pay in full at the end of the month, talk to your healthcare providers about the possibility of extending payments for, say, a year or more.

But what if you decide to gradually pay your medical bills using credit? "Shop around for the lowest interest rate, perhaps a fixed rate that will stay in effect for as long as you expect to be making payments," added Gray. "Also be aware that many healthcare providers have arrangements with certain lenders to promote their loans and credit cards for medical debts, so do some research to find the card that's best for you. Don't turn to the provider's recommended form of credit just because it appears to be the easiest way to pay."

Only use your home to finance medical bills as a last resort. Home equity loans enable you to borrow money against your home's value to pay for major expenses, including medical debts, and perhaps qualify for a tax deduction on the interest payments. But remember that if you borrow using a home equity product, and you cannot make the loan payments, you could lose your home.

"Your house is a valuable asset," said Luke W. Reynolds, Chief of the FDIC's Community Outreach Section. "You should think very carefully before putting your home on the line to finance medical debts."

Be very careful before withdrawing money "early" from your retirement savings to pay for medical expenses. Taking funds from an Individual Retirement Account (IRA) before age 59½ sometimes can trigger sizeable tax penalties. Also, the more money you take out of IRAs, 401(k) accounts and other retirement plans before retirement, "the less you will have available for other needs during retirement, plus you will lose out on the ability of the funds to compound and grow," said Reynolds.

Contact the doctor's office or hospital immediately if you don't think you can pay a medical debt. Explain your situation and try to negotiate the bill or offer a reasonable payment plan before it is referred to a collection agency.

Before putting your financial future at risk by taking an early withdrawal from an IRA, ask your healthcare provider about a realistic repayment plan.

Don't be afraid to ask for additional help. Depending on your age or income level, you may qualify for aid in handling medical debts under the federal Medicaid program or state government initiatives. Many hospitals offer free or discounted care for patients who don't qualify for government programs and meet specific financial criteria. Most hospitals also have financial counselors who can help patients understand the various programs and help with applications.

In addition, a reputable credit counseling service may be able to help consumers get their medical debts under control. And, if you have medical bills that have been sent to collection, you may negotiate to reduce the bills and pay them through an installment plan.

For information about how to deal with debt problems in general, including how to avoid problems with debt collectors and find reliable credit counseling, visit the consumer facts Web page from the Federal Trade Commission at www.ftc.gov/bcp/menus/consumer/credit/debt.shtm.

Ideas for Growing a Small Business

Tips on getting loans and managing money

Are you one of the millions of small business owners in the United States? Or are you considering starting your own company? Just as with consumers, it's important for small business owners to make sound financial decisions so they can grow and prosper. ***FDIC Consumer News*** offers these tips for small business owners on topics ranging from financing your operations to managing your accounts.

Get a head start with business experts who can help you. The U.S. Small Business Administration (SBA) provides education and counseling through a variety of programs and partners. The SBA's help includes online training, Web chats for small business owners, and referrals to local classes and confidential counseling. Topics range from writing a business plan to qualifying for a loan. Check with your SBA district office or visit www.sba.gov.

In addition, don't hesitate to ask a banker for advice on financing and interest rates and for referrals to other local resources that can help you build your business. It also can pay to use the services of a small business counselor or attorney to make sure you comply with licensing, tax, insurance or other regulatory requirements. Other topics to address include the pros and cons of different ownership structures (such as becoming incorporated) and when you may need to request an employer identification number (EIN) from the Internal Revenue Service.

Establish a positive track record for your business. Just as credit bureaus maintain a record of your personal credit history, companies track how businesses handle their finances. "One way to establish and maintain a good credit history for your business is to make timely payments to your suppliers and vendors in the company's name," said Luke W. Reynolds, Chief of the FDIC's Community Outreach Section. "This can pay off when applying for a bank loan or negotiating how quickly you have to pay suppliers." Lenders also will likely review your personal credit report as an indicator of whether a business you own will repay a loan promptly.

Do your research to get the right loans at the right time. Whether you're just starting a small business or expanding to take advantage of new opportunities, obtaining financing can be vital to building a strong and thriving organization. The SBA is committed to helping small businesses obtain financing. Working closely with a wide range of lending partners across the country, the SBA has a variety of programs that address the borrowing needs of small businesses. For more information about SBA loan programs, visit www.sba.gov.

Be careful with credit cards for your company. "Interest rates on credit cards are usually much higher than on business loans," said Ron Jauregui, an FDIC Community Affairs Specialist. "So if you do decide to finance your company using credit cards, make sure you know the APR — the Annual Percentage Rate — and other key terms of the card."

Also, he said, if you plan to use a credit card for business expenses, consider obtaining a card in your company's name. Doing so will help you keep track of those expenses. And, for big-ticket business expenses (such as costly equipment) that you don't plan to pay in full by your credit card's due date, consider a bank loan at a lower interest rate instead of financing it at the credit card's higher interest rate.

Take advantage of the different banking services available. If you don't already have a checking account for your business, consider opening one. A bank account will help you record and monitor business expenses and ensure that the cash is safe from

continued on next page

FDIC
Consumer News

Published by the Federal Deposit Insurance Corporation

Sheila C. Bair, *Chairman*

Andrew Gray, *Director, Office of Public Affairs (OPA)*

Elizabeth Ford, *Assistant Director, OPA*

Jay Rosenstein, *Senior Writer-Editor, OPA*

Mitchell Crawley, *Graphic Design*

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

Send your story ideas, comments, and other suggestions or questions to: Jay Rosenstein, Editor, ***FDIC Consumer News,*** 550 17th Street, NW, Washington, DC 20429 jrosenstein@fdic.gov.

Find current and past issues at www.fdic.gov/consumernews or request paper copies by contacting the FDIC Public Information Center. Call toll-free 1-877-ASK-FDIC (1-877-275-3342), write to the FDIC Public Information Center, 3501 North Fairfax Drive, Room E-1002, Arlington, VA 22226, or e-mail publicinfo@fdic.gov.

Subscriptions: To receive an e-mail notice about each new issue with links to stories, go to www.fdic.gov/about/subscriptions/index.html. To receive ***FDIC Consumer News*** in the mail, free of charge, call or write the FDIC Public Information Center as listed above.

For More Help or Information

Go to www.fdic.gov or call the FDIC toll-free at 1-877-ASK-FDIC (1-877-275-3342)

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

10%
PRINTED ON RECYCLED PAPER

continued from previous page

loss or theft. "Even if you already have a business account, occasionally do some comparison shopping to ensure you are getting a deal that makes sense to you," advised Reynolds.

Some institutions may also offer software or other tools that allow you to deposit checks remotely over the Internet. (For more information, see the box on Page 3.) Institutions also often provide options to pay employees via direct deposit, which can save your business money and time compared to issuing paper checks.

Understand the FDIC's insurance coverage for your business deposits. Money that your business has on deposit with a bank is insured separately from your personal accounts at the same institution if the funds are in an account opened in the name of a corporation, partnership or other legal entity. But if you operate your business as a sole proprietorship, your business' funds are insured together with your personal deposits at that same institution in the "single account" category (those in your name alone and not including certain Individual Retirement Accounts), rather than being insured separately. However, if a sole proprietorship uses an account owned by two people — typically a husband and wife — "the FDIC would insure their business accounts under the 'joint account' category along with any other funds they own together at the same bank that are joint accounts," advised Martin Becker, an FDIC Senior Deposit Insurance Specialist.

Under current law, through year-end 2013, the maximum total FDIC deposit insurance coverage is $250,000 for single accounts, $500,000 for joint accounts (up to $250,000 for each owner's share), and $250,000 for business accounts. For more details, see the FDIC resources on deposit insurance at www.fdic.gov/deposit/deposits or call toll-free 1-877-ASK-FDIC, which is 1-877-275-3342.

Take steps to protect your small business from online fraud. The FDIC has seen an increase in reports of unauthorized electronic transfers made from bank accounts held by small businesses. "Most of the incidents occurred because the small business' online banking IDs and passwords were compromised," said Kathryn Weatherby, a fraud specialist at the FDIC. "This may happen when a small business owner's computer becomes infected with malicious software — often called malware — that logs the keystrokes of the person at the computer and records valuable information."

To protect against malware and other online threats, Weatherby said, small businesses should ensure that their internal networks are secure and that their anti-virus and security software is up to date. They also should monitor and reconcile accounts frequently, perhaps even daily, and immediately report unusual activity to their financial institution. For more information about Internet security that small businesses may find useful, see Pages 2 through 4.