Winter 2005/2006

FDIC Consumer News

Fires, Floods and Other Misfortunes: Are You Prepared Financially?

Be ready to conduct daily money matters after a disaster

What items to keep at home… and what to store elsewhere

How to avoid fraudulent charities and other scams

Also Inside

FEDERAL DEPOSIT INSURANCE CORPORATION

Fires, Floods and Other Misfortunes: Are You Prepared Financially?

Disasters can impair your ability to conduct day-to-day money matters. This guide can help you plan appropriately.

While Hurricane Katrina was the dominant disaster story in the U.S. in 2005, other calamities such as floods, fires, earthquakes, tornadoes, hurricanes or similar events occur frequently, forcing people to evacuate their homes. Minor disasters also damage or destroy property or personal belongings. Just ask anyone whose has had a water pipe burst at home, turning their storage or living space into a wading pool. So why is the FDIC — a banking regulator — telling you about floods and fires?

Because natural or man-made disasters strike without warning and can happen to anyone. They can also seriously impair victims' ability to conduct essential financial transactions.

Certainly, your first concerns in an emergency should be your safety and basic needs such as shelter, food and water. But you also should be ready to deal with financial challenges, such as how to pay for supplies or temporary housing, if necessary.

"Being prepared to function financially if you have to leave your home at a moment's notice will give you less to worry about if an unfortunate event happens to you," said Janet Kincaid, FDIC Senior Consumer Affairs Officer.

What about you? If you had only a few moments to evacuate your home — and were away for several days or even weeks — would you have access to cash, banking services and the personal identification you need to conduct your day-to-day financial life? Here are some tips from the FDIC, based in part on our recent experience staffing a 24-hour call center to respond to banking-related questions from victims of Hurricanes Katrina and Rita.

What to Have Ready

Consider keeping the following documents, bank products and other items in a secure place and readily available in an emergency. (For guidance on how and where to keep originals and copies of selected items, keep reading.)

Forms of identification: These primarily include driver's licenses (or state ID cards for non-drivers), insurance cards, Social Security cards, passports, and birth certificates. These documents will be crucial if you or your family should need to rebuild lost records or otherwise prove to a government agency, a bank or other business that you are who you claim to be. "It's best to have the originals, but it's also important to have photocopies of these documents in case originals are misplaced or destroyed," said Kincaid. "Also, never keep the originals with the copies."

Your checkbook with enough blank checks and deposit slips to last a month or so: Your need for checks will vary depending on how long you may be displaced or how often you write checks. Even if you rarely or never write checks, at least consider having a copy of a check or your checking account number handy. That's because, in an emergency, you can authorize an important payment by providing the recipient (for example, an insurance company) your checking account number over the phone.

Automated teller machine cards, debit cards (for use at ATMs and merchants) and credit cards: These cards give you access to cash and the ability to make payments on outstanding bills. Most ATM and debit cards require the use of personal identification numbers (PINs), so make sure you know

those numbers. Don't write your PINs on or near your cards in case they are lost or stolen. Also, don't assume that merchants and ATMs in areas affected by a disaster will be immediately functioning as usual — that's why it's smart to have other options available for getting cash and making payments, as described in this article.

Cash: The amount you should have available will depend on several factors, including the number of people in your family and your ability to use ATM, debit and credit cards to get more cash or make purchases. But remember that cash in your house or wallet and not in your bank account can easily be lost or stolen.

Phone numbers for your financial services providers: These would include local and toll-free numbers for your bank, credit card companies, brokerage firms (for stocks, bonds or mutual fund investments) and insurance companies. Why have these numbers handy? You may need to defer a payment, replace lost cards or documents, open new accounts, or otherwise request assistance. If you have people you regularly deal with, have their phone numbers on your list, too. "Working with someone who knows you can speed things up and provide you with some additional peace of mind," said Kincaid.

While Hurricane Katrina was the dominant disaster story in the U.S. in 2005, other calamities such as floods, fires, earthquakes, tornadoes, hurricanes or similar events occur frequently, forcing people to evacuate their homes. Minor disasters also damage or destroy property or personal belongings. Just ask anyone whose has had a water pipe burst at home, turning their storage or living space into a wading pool. So why is the FDIC — a banking regulator — telling you about floods and fires?

Because natural or man-made disasters strike without warning and can happen to anyone. They can also seriously impair victims' ability to conduct essential financial transactions.

Certainly, your first concerns in an emergency should be your safety and basic needs such as shelter, food and water. But you also should be ready to deal with financial challenges, such as how to pay for supplies or temporary housing, if necessary.

"Being prepared to function financially if you have to leave your home at a moment's notice will give you less to worry about if an unfortunate event happens to you," said Janet Kincaid, FDIC Senior Consumer Affairs Officer.

What about you? If you had only a few moments to evacuate your home — and were away for several days or even weeks — would you have access to cash, banking services and the personal identification you need to conduct your day-to-day financial life? Here are some tips from the FDIC, based in part on our recent experience staffing a 24-hour call center to respond to banking-related questions from victims of Hurricanes Katrina and Rita.

What to Have Ready

Consider keeping the following documents, bank products and other items in a secure place and readily available in an emergency. (For guidance on how and where to keep originals and copies of selected items, keep reading.)

Forms of identification: These primarily include driver's licenses (or state ID cards for non-drivers), insurance cards, Social Security cards, passports, and birth certificates. These documents will be crucial if you or your family should need to rebuild lost records or otherwise prove to a government agency, a bank or other business that you are who you claim to be. "It's best to have the originals, but it's also important to have photocopies of these documents in case originals are misplaced or destroyed," said Kincaid. "Also, never keep the originals with the copies."

Your checkbook with enough blank checks and deposit slips to last a month or so: Your need for checks will vary depending on how long you may be displaced or how often you write checks. Even if you rarely or never write checks, at least consider having a copy of a check or your checking account number handy. That's because, in an emergency, you can authorize an important payment by providing the recipient (for example, an insurance company) your checking account number over the phone.

Automated teller machine cards, debit cards (for use at ATMs and merchants) and credit cards: These cards give you access to cash and the ability to make payments on outstanding bills. Most ATM and debit cards require the use of personal identification numbers (PINs), so make sure you know those numbers. Don't write your PINs on or near your cards in case they are lost or stolen. Also, don't assume that merchants and ATMs in areas affected by a disaster will be immediately functioning as usual — that's why it's smart to have other options available for getting cash and making payments, as described in this article.

Cash: The amount you should have available will depend on several factors, including the number of people in your family and your ability to use ATM, debit and credit cards to get more cash or make purchases. But remember that cash in your house or wallet and not in your bank account can easily be lost or stolen.

Phone numbers for your financial services providers: These would include local and toll-free numbers for your bank, credit card companies, brokerage firms (for stocks, bonds or mutual fund investments) and insurance companies. Why have these numbers handy? You may need to defer a payment, replace lost cards or documents, open new accounts, or otherwise request assistance. If you have people you regularly deal with, have their phone numbers on your list, too. "Working with someone who knows you can speed things up and provide you with some additional peace of mind," said Kincaid.

Important account numbers: These would include bank and brokerage account numbers, credit card numbers, and homeowner's or renter's insurance policy numbers. Kincaid also suggests copying the front and back of your credit cards (and keeping them in a safe place). "Often times, if you have a copy of your credit card and a valid ID, you can make a purchase without having your actual card," she explained. Plus, the photocopies can help you keep track of your account numbers and company phone numbers.

The key to your safe deposit box: You can't get into your safe deposit box at the bank without your key, no matter how many forms of identification you have. Also, while many banks issue two keys when a box is rented, simply giving someone else a key doesn't allow that person access to a box in an emergency. He or she also must be designated in the bank's records as a joint renter or be appointed a "deputy" or "agent" who has access to your box. Contact your bank about the proper arrangements.

What to Keep Where

After you've gathered your most important financial items and documents, protect them as well as you can, while also ensuring you have access to them in an emergency. Here's a reasonable strategy for many people:

Make backup copies of important documents. You'll want duplicates for

Consumer Alert: Beware of Disaster-Related Financial Scams

Disasters such as the tsunami in 2004 and the hurricanes in 2005 can bring out the best in some people and the worst in others, including fraud artists.

"Criminals may take advantage of a bad situation by preying on peoples' fears, sympathy and desire to help others who have suffered disastrous hardships," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "For example, following catastrophic events we usually see a spike in reports of fake Web sites and fraudulent phone calls or e-mails claiming to be from legitimate charitable organizations that, in reality, may be criminals pocketing donations that were intended to go to disaster victims."

Other rip-off artists, according to a warning from the Federal Trade Commission (FTC), descend on damaged areas and offer to repair or restore homes but "overcharge, perform shoddy work or skip town without finishing your job."

You can avoid becoming a victim by taking these precautions:

Don't give cash. Use either a check or a credit card, so that you have some consumer protection, such as placing a hold on a check or disputing the transaction with the credit card company.

Protect your personal and financial information. Never divulge bank or credit card numbers or other personal information in response to an unsolicited call, e-mail, fax or knock at the door, no matter how official or legitimate the request may appear to be.

Give only to charities that you know or you have researched thoroughly. Resources include your state government office that regulates charities (usually part of the Attorney General's office or check the Web site of the National Association of State Charity Officials at www.nasconet.org/agencies), the IRS list of charities that are eligible to receive tax-deductible donations (www.irs.gov/charities/index.html) and the Better Business Bureau, which maintains reports on national and local charities (in your phone book or online at www.give.org).

Take special precautions when considering an online donation. Go directly to a charity's Web site by independently confirming the correct Internet address. Don't follow a link from one Web site to another because the link may be to a fake Web site operated by scam artists, even though it may look identical to the real Web site. Also, Benardo warned, "sometimes those links enable criminals to monitor your computer for credit card numbers and passwords that they can use to drain your accounts."

Check out any unsolicited offers of repairs or other products or services for disaster victims. For example, the FTC says to deal only with licensed and insured home-repair contractors, get recommendations from people you know and trust, and check with the local Better Business Bureau for any record of complaints. Also get prices and other key details in writing and take your time before signing a contract.

Remember the red flags of a fraud. Trust your judgment if something just doesn't seem right or makes you feel uncomfortable. Here are examples of situations in which your best response may be to walk away or hang up:

- You're being pressured to act quickly, perhaps to send money or provide personal information on the spot.
- You're told you already agreed to donate or pay money, and you don't remember doing so.
- An organization uses a name or Web site that sounds or looks like that of a well-known, respected charity, but on closer examination it's not the same.
- Someone claims to be a disaster victim and asks for your help in placing funds in an overseas bank account.

Report suspected frauds. Go to www.lookstoogoodtobetrue.com/complaint.html, a Web site co-sponsored by the FBI and the U.S. Postal Inspection Service, to file a complaint. You can also contact the FTC toll-free at 1-877-FTC-HELP (1-877-382-4357).

Banks Are Required to Prepare for Disasters

Federal and state banking regulators require financial institutions to develop and test "disaster recovery" and "business continuity plans." Each plan must spell out how the bank will recover data, ensure the availability of cash, continue customer service, and otherwise function efficiently after a wide-ranging disaster — one in which personnel are unavailable, key facilities are closed, and power and phones are out for an extended period.

According to Michael Jackson, an Associate Director of the FDIC's Division of Supervision and Consumer Protection, the terrorist attacks on September 11, 2001, and the recent devastation from Hurricanes Katrina and Rita reminded the financial industry and its regulators "that you must be ready for a disaster of any magnitude or duration — you cannot plan for something small or brief."

"Banking institutions play a vital role in supporting the economy, businesses and individual families after a disaster," added Kathryn Weatherby, an Examination Specialist for the FDIC. "It's in everyone's best interest that banks bounce back quickly and that disruptions are minimized."

Safe Online Banking, Shopping and Bill Paying: Our Latest Tips on Services Protecting Consumers

Helping consumers safely bank, shop and pay bills online has been a priority for the FDIC for many years. We closely watch the Internet for new risks and periodically issue guidance to bankers and warnings to consumers about precautions they can take to support safe online banking activities. Now, based on recent FDIC studies and a series of conferences held across the country to discuss identity theft, here are our latest suggestions for products or services to consider for protecting yourself online. (Not all financial institutions offer each product or service described here so it's up to you to find the solution that works for you.)

Protecting Card Numbers

"Credit card numbers are a cyber criminal's most attractive target," said David Nelson, a fraud specialist in the FDIC's Division of Supervision and Consumer Protection. "Stolen card numbers can be used to make counterfeit cards and run up big charges on your account." Some new options to consider for protecting your credit card number include:

Single-use credit card numbers: Also known as "virtual cards," these are numbers issued by your bank or credit card company for one-time use with online purchases and catalog or phone orders. "By using a one-time account number, you get peace of mind knowing that your actual credit card number isn't revealed to the merchant and can't be stolen by a crook," said Nelson. "Plus, each number can only be used with one merchant, so it will be void if someone tries to use it elsewhere." Your authorized charges using a one-time number will show up on your monthly statement, just like any other purchase.

Password protection: When making a purchase online you must enter a password along with your credit card number. So far, this extra security measure is only available for online purchases at merchants that participate in the program. However, more and more merchants are making this security feature available.

Online credit card statements and account access: You may not realize it, but the ability to use your computer to check your credit card balance, receive alerts and monthly statements and pay your card bill online offers you ways to protect against identity theft, too. Examples: If your credit card issuer sends you periodic e-mails with current balance and payment information, you can look for suspicious transactions. When you get an e-mail saying your monthly statement is available online to view or print, this arrangement may replace the traditional mailing of your credit card statement and thus prevent the information from being lost or stolen. The e-mail alert, which will include part of your account number or some other sign of authenticity, links you to a secure connection that is encrypted and requires a password for access.

And if you don't have access to a computer or your computer isn't working, you may be able to make your card payments and get credit card account information electronically using your telephone.

Protections for Online Banking

Here are protections some banking institutions are offering to help consumers guard against errors or unauthorized transactions online:

Guaranteed bill payment: If your bank makes an error and an online bill payment arrives late, this service would cover any late fees.

Online authentication: Banks are coming up with new, innovative ways to identify their real customers from impersonators in Internet transactions.

FDIC Web Presentation: How to Prevent Online ID Theft

With identity theft continuing to be one of the fastest-growing, most sophisticated crimes in the United States, the FDIC has posted on its Web site an audio-visual presentation to help consumers protect against ID theft that originates online. Entitled "Don't Be an Online Victim," the tutorial explains how to guard against Internet thieves and electronic scams, including protections for your computer and what to do if you believe you've been victimized. To see the program online, go to the FDIC's Web site www.fdic.gov/consumers/consumer/guard/index.html.

Don't be surprised if, as part of the online banking process, you are asked to verify something that you know but a crook wouldn't. (For more information, see the next page.)

Avoiding Fraudulent Sites

There are numerous high-tech scams aimed at accessing your bank account online. In one example, known as "pharming," a computer virus or other malicious program redirects your PC to a fraudulent bank or retail Web site. The crooks behind the Web site collect your personal information for use in fraud and identity theft. The following services can help you:

The "padlock" symbol of certification: Before you enter personal information when banking or buying online, look for the image of a padlock on the lower part of your computer screen, double click on it, and read the certification information on the pop-up screen. It tells you who you are dealing with and that you are on a secure site certified by a trusted third party. "If there is no padlock," said Nelson, "you can't be sure who

continued on next page

owns the Web site and how your information is protected in transit, and that means you are taking on more risk."

Verification engines: As an alternative to clicking on a padlock, you can install software onto your computer that will automatically tell you if a Web site you are visiting is real or fake. "Verification engines do the security work for you," said Robert Lee, a technology specialist in the FDIC's Division of Supervision and Consumer Protection.

Countering "Spyware"

Spyware refers to malicious programs that can get onto your computer in numerous ways, including when you open e-mail attachments or "instant messages," listen to music or watch videos online. Inside your system, spyware can secretly change your security settings and record your keystrokes. By doing so, the criminals can steal personal information (such as passwords or credit card numbers you've typed) that can be used to gain access to your bank account.

While spyware can be difficult to guard against, you can improve your chances by adding a "firewall" (to stop hackers from accessing your computer) and installing and periodically updating virus protection (to block and detect spyware). Some of these and other services can be found for free on the Internet. "Be selective because some products claiming to be anti-spyware software *actually are* spyware," said Aurelia Cardamone, a Senior Technology Specialist in the FDIC's Division of Supervision and Consumer Protection.

Nelson also suggests that you consider moving sensitive personal or financial records, such as tax returns or bank statements, from the hard drive of your computer onto diskettes or CDs that spyware can't access. "If the data are not stored on your computer, hackers can't find, copy, transmit, store and sell it," he said. "Just make sure you keep the diskettes or CDs in a safe place." 🏛

Coming Soon to Internet Banking Customers: New Procedures for Verifying that "You are You"

The latest in the federal government's fight against online fraud

FDIC Consumer News has warned readers for years to be on guard against fraudulent e-mails and Web sites that try to trick you into revealing confidential information, such as bank passwords, that can be used to steal money from accounts. Now we want to let you know about new recommendations from federal regulators (including the FDIC) intended to help banking institutions differentiate their true customers from fraud artists and to help Internet users recognize real bank Web sites from fraudulent sites.

In general, the guidelines — which are based in part on an FDIC study released in December 2004 — recommend that each federally insured bank, savings institution and credit union do the following by year-end 2006:

Analyze its Internet services in terms of the potential for fraud or theft. Some bank Web sites only provide details such as branch locations and interest rates on products, which are low-risk activities. But Internet-based banking services that can move money out of accounts or permit Internet users to access confidential information (such as Social Security and bank account numbers) are considered at high-risk for attempted fraud or identity theft.

Ensure that high-risk Internet services are protected by more than just passwords. Possible options include low-tech solutions, such as the use of questions and answers that only your bank and you know, and "scratch cards" with special passwords that are provided to account holders for one-time use. However, there also are high-tech identification programs that include special devices, such as:

- A "token" provided to customers that will generate a unique access number for use with each Internet transaction;
- A "smart card" that is similar to an automated teller machine (ATM) access card but for the Internet;
- A pre-arranged, customer-chosen picture or image that would appear every time you want to perform an

For More Information About Preventing Internet Fraud

The **FDIC Web site** at www.fdic.gov features brochures, consumer alerts and articles published in ***FDIC Consumer News*** on topics such as safe banking over the Internet and protecting against identity theft online. You can also watch an FDIC video about protecting against online scams.

OnGuard Online is a Web site that has tips from the federal government and the technology industry to help consumers protect against Internet fraud, secure personal computers and avoid ID theft. The site, which is maintained by the Federal Trade Commission (FTC), can be found at onguardonline.gov.

The **FTC's Web site** also has a wide assortment of consumer information on topics such as shopping and paying safely online and avoiding ID theft. Start at ftc.gov/consumer.

The new **"Looks Too Good To Be True" Web site**, a joint effort of federal law enforcement agencies and corporate partners, is intended to educate consumers on how to avoid Internet frauds. The site, which is funded by the United States Postal Inspection Service and the FBI, is located at www.lookstoogoodtobetrue.com.

New federal guidelines recommend that each institution ensure that high-risk Internet services are protected by more than just passwords.

online transaction, assuring an Internet customer that he or she had reached the bank's real Web site and not an impostor site;

• A "digital certificate" — a high-tech seal of approval from an online security service — that confirms the identity of an Internet user in a transaction with a bank or merchant.

• Software to recognize the real customer's fingerprint, voice or even their typical keystroke patterns.

If your institution adds new authentication methods for certain Internet products or services, your bank will notify you, perhaps in your monthly statement or in an e-mail.

But what if your bank doesn't tell you about any enhanced security measures? "It may be that your bank already uses enough other ways to authenticate you as a customer, including some behind the scenes," said Michael Jackson, an Associate Director of the FDIC's Division of Supervision and Consumer Protection. Possible examples, he said, include systems that enable a bank to confirm that a request is originating from your home computer and not someone else's, and maximum dollar limits on certain transactions that need special approval to be done online.

Jackson also noted that federal examiners will review each institution's assessment of its online banking risks as well as the security measures in place to make sure they satisfy government guidelines. 🏛

Update on FDIC Insurance

Increase in $100,000 Limit Under Consideration for Retirement Accounts

As ***FDIC Consumer News*** went to print, Congress was close to adopting legislation that would raise the federal insurance limit for certain retirement accounts (Individual Retirement Accounts and other retirement accounts for which you choose the FDIC-insured bank or thrift that gets the deposit) from $100,000 to $250,000. Under the pending legislation, coverage limits for all other consumer accounts would NOT be changed — the standard insurance limit would remain at $100,000 per depositor. Any changes in the insurance rules and their effective dates will be noted on the FDIC Web site at www.fdic.gov.

Expanded FDIC Insurance for College Savings Accounts

A new rule from the FDIC provides that people who place "529-plan" college savings into bank deposits are better protected against loss if the bank were to fail. State-sponsored 529 plans (named after section 529 of the Internal Revenue Code) are tax-advantaged accounts that help families and individuals save for higher education expenses. Under the new rule, deposits that a 529-plan administrator places at a bank on behalf of many different individuals are federally insured up to $100,000 for each participant, not to $100,000 for all of the participants combined. While most states don't allow participants to have their 529-plan money placed in bank deposits — they instead limit the choices to investments such as stocks and bonds — several states have begun adding bank deposits as an option. The rule took effect December 27, 2005.

FDIC
Consumer News

Published by the Federal Deposit Insurance Corporation

Martin J. Gruenberg, *Acting Chairman*

DJ Nordquist, *Director, Office of Public Affairs (OPA) and Deputy Chief of Staff*

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 newsletter may be reprinted in whole or in part. Please credit ***FDIC Consumer News***.

Send comments, suggestions or questions to: Jay Rosenstein, Editor, ***FDIC Consumer News***
550 17th Street, NW, Room 7100
Washington, DC 20429
jrosenstein@fdic.gov

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

To receive an e-mail notice about each new issue with links to stories, follow instructions posted at:
www.fdic.gov/about/subscriptions/index.html.

For More Information from the FDIC

Go to www.fdic.gov or call toll-free 1-877-ASK-FDIC — that's 1-877-275-3342 — Monday through Friday 8:00 a.m. to 8:00 p.m., Eastern Time.

Reminder: Deposited Checks Subject to Temporary "Hold"

Federal rules allow banking institutions to put a temporary "hold" on certain deposits as a way of protecting against losses, primarily from checks drawn against accounts with insufficient funds. Depending on the type of deposit — electronic direct deposit, Treasury check, local check, large check and so on — you may have to wait anywhere from one business day to 11 business days before you can withdraw your deposit. Many consumers do not understand when their deposited funds can be made available to them. To raise awareness of the rules, we are providing responses to two common questions consumers have about holds on checks.

I deposited into my bank account in Maine a $6,000 check drawn on a bank in Texas. The next day, I received a notice from my bank that part of my deposit was being held for 11 business days because it is a "large deposit." Is my bank allowed to do this?

Yes. Federal Reserve Board (Fed) rules governing funds availability permit a bank to hold a large check ($5,000 or more) for up to seven business days if it's a local check and up to 11 business days if it's a non-local check.

First, be aware that $100 of the deposit must be made available after one business day as a way of getting some of the funds to you quickly. In addition, the bank must make the first $5,000 of the deposit available for withdrawal according to the bank's policy for non-local checks (which should be no later than the fifth business day after the deposit). For the remaining $1,000 of the $6,000 deposit, the bank is permitted under the rules to withhold the money up to 11 business days. The rules issued by the Fed also specify how and when you must be informed of the hold being imposed.

A friend says that her bank never places a hold on her deposited checks. My bank always places holds on my checks. Aren't banks supposed to use the same schedule for making funds available?

No. While all banks are subject to the same *maximum* hold periods established by law and the rules issued by the Fed, each bank may make deposits available sooner. Each bank determines what its policy will be. It can make all of the funds available immediately or delay availability up to the maximums permitted by law. There is no requirement that banks uniformly provide the same availability schedule.

Finally, if you need funds from a deposit quickly or if you're unsure about your bank's check-hold policies, talk with a manager at your bank. For more information about the rules governing funds availability, see a guide (primarily for financial institutions) posted on the Fed's Web site at www.federalreserve.gov/pubs/regcc/regcc.htm. You can also call 1-202-452-3693, send an e-mail to www.federalreserve.gov/feedback.cfm or write to the Federal Reserve Board, Division of Consumer and Community Affairs, 20th Street and Constitution Avenue, NW, Mail Stop 801, Washington, DC 20551.