



New Credit Card Rules and the Latest in Fraud Scams

This month's column highlights some of the latest fraudulent scams being perpetrated against an unsuspecting public. However, with the enactment of new credit card rules effective February 22, 2010, this is also a good time to remind you of some new consumer protections including:

- You may cancel your card before the credit card company changes the terms of your account.
- Rate increases are prohibited during the first year after an account is opened and that prohibition also applies to an existing credit card balance.
- Creditors are prohibited from issuing a credit card to anyone younger than 21 years of age unless the consumer has the ability to make the required payments or obtains a signature of a cosigner who has the ability to make the required payments.
- A consumer's consent is required before charging fees for transactions that exceed the credit limit.
- Creditors can no longer use the "two-cycle" billing method to impose interest charges.
- Creditors cannot allocate payments that maximize interest charges.

For more information, log on to The Federal Reserve at <http://www.federalreserve.gov> for the online publication entitled "What You Need to Know: New Credit Card Rules".

Consumer Scams

Criminal scams continue to plague consumers. Here are three of the most common scams being committed on consumers, and recommendations on how to avoid getting ripped off. Read on for more information about the latest scams as reported by the Better Business Bureau and FBI.

Natural disaster relief fraud – From hurricanes to tsunamis to earthquakes, the past few months and years have brought us many deadly and heartbreaking natural disasters. When a natural disaster strikes, generous donations to charities are necessary to relieve the suffering, but these disasters also bring out criminals. These criminals are often disguised as worthwhile charities, but their only goal is to relieve you of your hard-earned money. Many of these scam artists are soliciting donations by telephone and email. Most recently, these criminals are asking for charitable donations to support relief efforts in Haiti. Tips to avoid getting ripped off:

- Hang up the phone or delete the emails asking for charitable donations. Contact your favorite charity directly to ask them what they are doing for the most recent natural disaster.
- Beware of calls and emails from charities using names that are the same or similar as well-known charities.
- Don't be afraid to say "good bye" and hang up on anyone trying to persuade you into giving.

- Never give cash or give money to a courier.
- Write a check and get a receipt.
- Contact the American Institute of Philanthropy, which is a national charity watchdog that assists in identifying reliable charitable organizations. They are online at: www.charitywatch.org.

Federal grant scams – People are receiving telephone calls claiming that they have been selected by a government agency to receive thousands of dollars in free grant money that doesn't have to be repaid. The caller asks for bank account information to transfer the funds into an account. Tips to avoid getting ripped off:

- Don't give your bank account information to anyone you don't know.
- Don't agree to pay for anything that is "free."
- If you get a telephone call from a governmental agency and you want to investigate it, don't give the caller any information; look up the agency online or in the blue pages of your telephone book, and call them to ask about the offer.

Text messaging scams – With the phenomenal growth of text messaging, it was only a matter of time before scams appeared in texts. One scam involves a text message that impersonates your bank. Many people have received this text message: "Wachovia alert – your card starting with 4828 has been deactivated please contact us at 555-555-5555 to reactivate your card." The truth is, all Wachovia bank cards start with "4828." Similar text message and email scams also have posed as other financial institutions. Anyone calling the phone number provided is asked for personal banking information, which is used to steal money. Tips to avoid getting ripped off:

- If you do not know who is making a request for personal information, delete the message/email or hang up.
- Never give out personal information, such as your social security number, bank account numbers or credit card numbers, to anyone you do not know.
- Banks will never ask for personal account information by text message or email.
- If you receive a call asking for personal information, hang up and call your financial institution to verify that the request is valid.

This information is provided with the understanding that the association is not engaged in rendering specific legal, accounting, or other professional services. If specific expert assistance is required, the services of a competent, professional person should be sought.

Provided as a public service by the member banks of the Iowa Independent Bankers.