Jim Hegarty is president of the Better Business Bureau representing Nebraska and southwest Iowa. To contact him, email to jhegarty@bbbnebraska.org or call 402-898-8520.

Published Tuesday October 4, 2011

For many people, credit cards mean freedom from carrying cash and the security of knowing there's money available for emergencies. In these tight times, some people use credit cards to pay even for everyday expenses. It is no surprise that, in our stressed economy, credit card debt continues to be a significant problem for average American households.

Most people who accrue credit card debt hope to pay it off when they feel more financially flush, and a telephone offer of lower credit card interest rates would be a delightful surprise to many such folks. Unfortunately, sharing personal information — even with just one unscrupulous caller — sometimes leads to financial devastation.

Predators are always ready to pounce on the vulnerable, and, unfortunately, crooks are exploiting American consumers through our credit cards.

Scammers are contacting consumers randomly, hoping the individual or family will have some credit card debt. They promise to negotiate lower credit card interest rates on your behalf in exchange for exorbitant fees.

In reality, consumers can easily contact their credit card companies (for free) and try to negotiate interest rates, and callers like these often provide little or no actual help. Also, they tend to refuse to return fees when consumers' rates remain unchanged.

Sometimes the calls are from identity thieves who capitalize on people's anxieties about their debts by stealing personal information and driving their victims even further into financial ruin.

Oct. 17 marks the beginning of the Better Business Bureau's "Secure Your ID Week." Each October, the Bureau emphasizes the importance of consumers and businesses staying vigilant and safeguarding sensitive personal and financial information.

Better Business Bureaus and attorneys general across the nation are receiving daily complaints from consumers who are getting calls from criminals claiming to be representatives of legitimate financial institutions.

Personally, I have received several calls this month from people claiming to be Chase Bank's fraud department. They profess to be notifying me of suspicious activity on my Chase Credit Card.

I told one caller I wasn't a Chase cardholder. He apologized for the misunderstanding and began asking me for personal information so he could "get to the bottom" of why I was being incorrectly called. When I asked to speak to his supervisor, he hung up.

These callers, of course, were not actually from Chase Bank. They were hoping to glean sensitive information from me, such as my credit card number, my address, my mother's maiden name or my Social Security number.

This "mass contact" technique is referred to as "phishing." Criminals send mass emails and/or pop-up messages on computers, or engage in mass text messages and even actual telephone calls, like the ones I received. Computer-generated calling equipment (robo-calls) dramatically increase their access to consumers.

Then they impersonate legitimate companies, such as banks and other financial institutions, to deceive consumers into revealing their credit card numbers, passwords, and other personal information.

One current scam involves an interactive recording. The caller hears, "Your MasterCard account has been locked for security purposes" then instructions to "unlock" the account. People who have MasterCard accounts, of course, might follow the assigned steps, which include entering credit card information "to reactivate the card."

Similar swindles involve text messages to mobile devices that inform consumers their debit cards have been deactivated. The text includes instructions to call an 877 number to contact "security services to reactivate." Slick crooks answer the 877 number and ask callers to verify their security codes and PIN information.

An Omaha woman who fell for the scam reported that, within hours of accidentally revealing her personal information, hundreds of dollars was withdrawn from her account.

Do NOT fall prey to the caller offering to help you out of a financial bind or to fix a problem with your credit account. Behind the robo-calling machines are people who are robbing the defenseless. Don't be their next victim.

If you get a robo-call or a "phishing" text message, you can contact the Federal Trade Commission at 877-FTC-HELP (382-4357) at www.ftc.gov. This federal agency has oversight of deceptive solicitations and will be able to record your complaint.

If you have inadvertently provided your banking information, follow these steps:

1. Contact one of the three major credit bureaus and place a "one-call" fraud alert on your credit report:

>> Equifax: 800-525-6285, www.equifax.com or P.O. Box 740241, Atlanta, GA 30374-0241.

>> Experian: 888-397-3742, www.experian.com or P.O. Box 9532, Allen, TX 75013.

>> TransUnion: 800-680-7289, www.transunion.com, or Fraud Victim Assistance Division, P.O. Box 6790 Fullerton, CA 92834-6790.

You need to call only one of the three credit bureaus; the one you contact will contact the two other bureaus for you. This alert remains in your credit file for at least 90 days and requires creditors to contact you before opening any new accounts or increasing your credit limits.

2. Immediately examine your bank account for any suspicious activity. Check your statements to ensure nothing is out of the ordinary. Report any irregularities to your financial institution.

3. Contact the fraud departments of your credit card issuers or bank. These financial institutions can monitor your account for suspicious activity. You may also decide to cancel these accounts.

4. Order a copy of your credit report and look for unauthorized activity.

5. If there is unexplained activity on your credit report, place an "extended" fraud alert on your credit report. For this type of alert, you need to file a police report and provide a copy of it to one of the three major credit bureaus. An extended fraud alert can be placed on your credit file for seven years. This discourages thieves by prohibiting new credit cards and increases in credit limits.

6. Take care when disposing of bills and bank statements that might give thieves just what they need to rip you off. Shredding is recommended, and we'll even do it for you. The BBB's "Secure Your ID Week" culminates Oct. 22 with a document shredding event at 84th Street and West Dodge Road between 8 a.m. and noon. Individuals and businesses can bring up to three boxes or bags of documents, and Shred It Omaha destroys all documents on site.