Financial Institution Letters

Internet Banking Fraud

FIL-103-2004
September 13, 2004

TO: CHIEF EXECUTIVE OFFICER

SUBJECT: Interagency Informational Brochure on Internet "Phishing" Scams

Summary: *The federal financial institution regulatory agencies have jointly published an informational brochure to help consumers identify and combat Internet "phishing" scams.*

The federal banking, thrift and credit union regulatory agencies have published an informational brochure to assist consumers in identifying and preventing a new type of fraud known as "phishing."

The term "phishing" – as in fishing for confidential information – is a scam that encompasses fraudulently obtaining and using an individual's personal or financial information. In a typical case, the consumer receives an e-mail requesting personal or financial information; the e-mail appears to originate from a financial institution, government agency or other entity. The e-mail often indicates that the consumer should provide immediate attention to the situation described by clicking on a link. The provided link appears to be the Web site of the financial institution, government agency or other entity. However, in "phishing" scams, the link is not to an official Web site, but rather to a phony Web site. Once inside that Web site, the consumer may be asked to provide Social Security numbers, account numbers, passwords or other information used to identify the consumer, such as the maiden name of the consumer's mother or the consumer's place of birth. When the consumer provides the information, those perpetrating the fraud can begin to access consumer accounts or assume the person's identity.

The brochure explains the basics of "phishing," the steps consumers can take to protect themselves, and the actions that consumers can take if they become a victim of identity theft. The brochure is available in a downloadable form through the FDIC's Web site at http://www.fdic.gov/news/news/press/2004/pr9304b.pdf 3,268k (PDF Help) (large file format) or http://www.fdic.gov/news/news/press/2004/pr9304a.pdf 224k (PDF Help) (small file format).

For your reference, FDIC Financial Institution Letters may be accessed from the FDIC's Web site at http://www.fdic.gov/news/news/financial/2004/index.html . To learn how to automatically receive FDIC Financial Institution Letters through e-mail, please visit http://www.fdic.gov/about/subscriptions/index.html.

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection

# # #

Attachments: You Can Fight Identity Theft

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342 or 202-

416-6940).

You Can Fight Identity Theft

You Can Fight Identity Theft (large file format) - PDF 3,268k (PDF Help)
You Can Fight Identity Theft (small file format) - PDF 224k (PDF Help)

WARNING
Internet Pirates are Trying to Steal YOUR Personal Financial Information
Here's the Good News—YOU have the Power to Stop Them

There's a new type of Internet piracy called "phishing." It's pronounced "fishing," and that's exactly what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards.

In the worst case, you could find yourself a victim of identity theft. With the sensitive information obtained from a successful phishing scam, these thieves can take out loans or obtain credit cards and even driver's licenses in your name. **They can do damage to your financial history and personal reputation that can take years to unravel.** But if you understand how phishing works and how to protect yourself, you can help stop this crime.

Here's how phishing works:

In a typical case, you'll receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the e-mail may appear to come from a government agency, including one of the federal financial institution regulatory agencies.

The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The e-mail will then encourage you to click on a button to go to the institution's Web site.

In a phishing scam, you could be redirected to a phony Web site that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual Web site. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information. In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth.

In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother’s maiden name or your place of birth.

If you provide the requested information, you may find yourself the victim of identity theft.

How to Protect Yourself

1. Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you *should not* provide any information.

2. If you believe the contact may be legitimate, contact the financial institution yourself. You can find phone numbers and Web sites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified yourself.

3. Never provide your password over the phone or in response to an unsolicited Internet request. A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.

4. Review account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity.

You Can Fight Identity Theft – Here's How:

Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact.

Never click on the link provided in an e-mail you believe is fraudulent. It may contain a virus that can contaminate your computer.

Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information.

If you believe the contact is legitimate, go to the company's Web site by typing in the site address directly or using a page you have previously book marked, instead of a link provided in the e-mail.

If you fall victim to an attack, act immediately to protect yourself. Alert your financial institution. Place fraud alerts on your credit files. Monitor your credit files and account statements closely.

Report suspicious e-mails or calls to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.

What to do if you fall victim:

- Contact your financial institution immediately and alert it to the situation.
- If you have disclosed sensitive information in a phishing attack, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name. Here is the contact information for each bureau's fraud division:

  Equifax
  800-525-6285
  P.O. Box 740250
  Atlanta, GA 30374

  Experian
  888-397-3742
  P.O. Box 1017
  Allen, TX 75013

  TransUnion
  800-680-7289
  P.O. Box 6790
  Fullerton, CA 92634

- Report all suspicious contacts to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling **1-877-IDTHEFT**.

A message from the federal bank, thrift and credit union regulatory agencies
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation

National Credit Union Administration
Office of the Comptroller of the Currency
Office of Thrift Supervision

Last Updated 9/10/2004 webmaster@fdic.gov

What to do if you fall victim:

- Contact your financial institution immediately and alert it to the situation.
- If you have disclosed sensitive information in a phishing attack, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name. Here is the contact information for each bureau's fraud division:

  Equifax
  800-525-6285
  P.O. Box 740250
  Atlanta, GA 30374

  Experian
  888-397-3742
  P.O. Box 1017
  Allen, TX 75013

  TransUnion
  800-680-7289
  P.O. Box 6790
  Fullerton, CA 92634

- Report all suspicious contacts to the Federal Trade Commission through the Internet at **www.consumer.gov/idtheft**, or by calling **1-877-IDTHEFT**.

You *Can* Fight Identity Theft

Here's How:

Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact.

Never click on the link provided in an e-mail you believe is fraudulent. It may contain a virus that can contaminate your computer.

Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information.

If you believe the contact is legitimate, go to the company's Web site by typing in the site address directly or using a page you have previously book marked, instead of a link provided in the e-mail.

If you fall victim to an attack, act immediately to protect yourself. Alert your financial institution. Place fraud alerts on your credit files. Monitor your credit files and account statements closely.

Report suspicious e-mails or calls to the Federal Trade Commission through the Internet at **www.consumer.gov/idtheft**, or by calling **1-877-IDTHEFT**.

A message from the federal bank, thrift and credit union regulatory agencies

Board of Governors of the Federal Reserve System

Federal Deposit Insurance Corporation

National Credit Union Administration

Office of the Comptroller of the Currency

Office of Thrift Supervision

WARNING

Internet Pirates are Trying to Steal YOUR Personal Financial Information

Here's the Good News: YOU have the Power to Stop Them

There's a new type of Internet piracy called "phishing." It's pronounced "fishing," and that's exactly what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards.

In the worst case, you could find yourself a victim of identity theft. With the sensitive information obtained from a successful phishing scam, these thieves can take out loans or obtain credit cards and even driver's licenses in your name. **They can do damage to your financial history and personal reputation that can take years to unravel.** But if you understand how phishing works and how to protect yourself, you can help stop this crime.

Here's how phishing works:

In a typical case, you'll receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the e-mail may appear to come from a government agency, including one of the federal financial institution regulatory agencies.

The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The e-mail will then encourage you to click on a button to go to the institution's Web site.

In a phishing scam, you could be redirected to a phony Web site that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual Web site. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information.

In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth.

If you provide the requested information, you may find yourself the victim of identity theft.

How to Protect Yourself

1 **Never provide your personal information in response to an unsolicited request**, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you ***should not*** provide any information.

2 **If you believe the contact may be legitimate, contact the financial institution yourself.** You can find phone numbers and Web sites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet. The key is that ***you*** should be the one to initiate the contact, using contact information that you have verified yourself.

3 **Never provide your password over the phone or in response to an unsolicited Internet request.** A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.

4 **Review account statements regularly to ensure all charges are correct.** If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity.