

July 2011



Bank of  
Central Florida

Treasury Management

Volume 3

Hello Business Internet Banking Clients:

With some recent internet fraud articles and other incidences of attempted fraud this newsletter is a reminder about some of the scams that are circulating from miscreants.

### **NACHA Phishing Alert:**

The National Automated Clearing House Association (NACHA) continues to receive reports from individuals and companies receiving fraudulent emails that have the appearance of being sent from NACHA. At the end of this newsletter, there is an article about an actual breach that fortunately did not result in any losses due to quick action on the part of the client involved and the banks.

DO NOT OPEN any files from NACHA asking to verifying information/totals, etc. NACHA does not directly process any files and would not communicate with ACH originators or originating Banks to verify data. Any communication about file totals would come from Bank of Central Florida Treasury Management or Deposit Operations. Additional information can be found in the following link:

<http://www.nacha.org/news/newsDetail.cfm/RecentBusinessNewsID/220>

### **FDIC Alert:**

#### **E-mail Claiming to Be From the FDIC - July 14, 2011**

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports of fraudulent emails that have the appearance of being from the FDIC.

The emails appear to be sent from various "@fdic.gov" email addresses, such as "protection@fdic.gov," "admin@administration.fdic.gov," or "service@admin.fdic.gov."

The messages have various subject lines that read: "Update for your banking account" or "ACH and Wire transfers disabled," and "Banking security update."

The fraudulent emails are addressed to "Dear clients" and state "Your account **ACH and Wire transactions** have been **temporarily suspended** for your Security, due to the expiration of your security version. To download and install the newest Updates, follow this [link](#). As soon as it is set up, your transaction abilities will be fully restored."

The message concludes with, "Best regards, Online security department, Federal Deposit Insurance Corporation."

These emails and links are fraudulent and were not sent by the FDIC. Recipients should consider the intent of these e-mails as an attempt to collect personal or confidential information, or to load malicious software onto end users' computers. Recipients should NOT access the link provided within the body of the emails and should NOT, under any circumstances, provide any personal financial information through this media.

Financial institutions and consumers should be aware that other subject lines and modifications to the e-mails may occur over time. The FDIC does not directly contact consumers in this manner nor does the FDIC request personal financial information from consumers.



### What happens if a virus/malware does infect a user's computer?

The pattern seems to be that the user will be redirected to a fake site and asked to enter their id, password, and security information 3 or 4 times. Once the miscreants get what they need, then they will post a message that the site is down for servicing for some period of time from a few hours to 24 hours.

Here is further explanation from our processing company's IT fraud department:

The financial industry is seeing more and more of these types of Trojans that employ an element of a man-in-the-browser (MITB) attack coupled with fraudulent phishing scam site setup exclusively to steal personal information. These MITB Trojans have the ability to redirect victims to fraudulent sites and/or inject iframes locally when visiting a legitimate site thereby presenting you with a modified version of that site (Any information is then sniffed out typically to an IM session that miscreant is monitoring in real time). They are typically automated and targeted attacks that remain dormant while user visits other sites until a user visits a specific financial site, in which time the malware then is triggered (usually embedded within the browser process) and does its thing.

We have also seen many instances of this type of malware behavior where victim is redirected to a site that allows them to enter their credentials, does the standard three times and then a similar message appears for 24 hours stating that site is down – during that time the miscreant is usually getting this information in real time and is able to use the token information before it changes and successfully logon and complete fraudulent transactions while user goes away and tries again in 24 hours only to find that some fraudulent Wire/ACH took place during that time.

The key here is that most of these types of Trojans/malware are constantly released with new signatures and very small footprint and often times go undetected by antivirus/antimalware products.

### What to do?

- ✓ Check the URL if you are getting multiple error messages when attempting to log in – be sure it is [https://bcfl.ebankingservices.com/Auth/SignIn/BeB\\_SignIn.aspx?auth\\_data](https://bcfl.ebankingservices.com/Auth/SignIn/BeB_SignIn.aspx?auth_data) rather than a mocked up version. You will also see your picture and phrase after you have entered your user id and before you enter your password.
- ✓ Please know that the e-Banking sites will **not** be down for maintenance during normal business hours. However, if the site is down for any reason, you will receive the message and the log in screen will not be accessible. The message will appear before you receive a log in page.
- ✓ Have your IT department scan for and clean the computers of viruses, malware, and Trojans.
- ✓ Any questions or if you think it just looks strange – feel free to call or email: [treasurymanagement@bankofcentralflorida.com](mailto:treasurymanagement@bankofcentralflorida.com) and ask us.

We are happy to assist and will check out your site for unusual IP log-in addresses and such.



Published: Friday, Jul. 08, 2011

Updated: 11:23 am Friday, Jul. 08, 2011

### **Hacker tried to steal \$83,000 from Atascadero city bank account**

Wire transfers were triggered by virus in email, according to city manager

By Bill Morem | [bmorem@thetribunenews.com](mailto:bmorem@thetribunenews.com)

The city of Atascadero and Rabobank are investigating how a computer hacker managed to breach multiple levels of security in an attempt to steal \$83,000 in wire transfers from a city account at the bank.

According to City Manager Wade McKinney, the hacker sent a phony email ostensibly from the National Automated Clearing House Association (NACHA), which annually facilitates billions of electronic payments such as direct deposit and direct payment.

When a city computer tech opened the email, it released a virus that used the wire transfer system the city has with the bank to transfer funds to accounts at several banks across the country that the city has no dealings with.

NACHA's website says that since February, it has been "the victim of sustained and evolving phishing attacks in which consumers and businesses are receiving emails that appear to come from NACHA. The attacks are occurring with greater frequency and increased sophistication."

According to McKinney, this is what happened in Atascadero:

Five transfers happened July 1, with three of those transfers adding up to \$30,000 and going to Tinker Federal Credit Union in Oklahoma, which does not do business with the city. After credit union employees noticed and then flagged the irregular transfers, they called the city to inform it about the transfers. The money will now be returned to the city by the bank.

The two other transfers that day never went through because of invalid account numbers.

Another five unsuccessful attacks were mounted Tuesday. The transfers, some of which were caught by Rabobank, were directed to banks in California, Florida, Maryland and Pennsylvania. "We're still trying to uncover all the details," McKinney said, "but it looks like we got a virus in one of the computers, then when we connected with Rabobank for a wire transfer, it got mirrored and sent out other transfers. We're looking into how it got around all of the security measures."

No one has been arrested for the crime. The FBI is investigating the case.

Read more: <http://www.sanluisobispo.com/2011/07/07/1674648/atascadero-hacker-bank-account.html#ixzz1STRaEnLb>



## Treasury Management

**Bank of Central Florida**  
**5015 South Florida Avenue**  
**Lakeland, FL 33813**



Thanks very much for banking with Bank of Central Florida.

Nancy LaFountain, CTP  
Vice President  
Treasury Management  
Phone: 863-904-4122

You may also call our newest addition to the Treasury Management department, Linda Harkins, Treasury Management Specialist, at 863-226-4069.

Fax: 863-701-2767

E-mail: [treasurymanagement@bankofcentralflorida.com](mailto:treasurymanagement@bankofcentralflorida.com)