

Phishing Attack in Progress; Please Read Below and Act Accordingly

We have become aware that some of our clients are receiving phishing emails that reference recipients to click on a link that takes them to a mock site that we presently believe may install malicious software. This may be a serious threat.

Please alert your organization about this issue, and direct recipients of the attached email NOT to open it or, if they do, NOT to click on the link.

The phishing attack is contained in a fraudulent email identical or similar to the one that follows:

-----Original Message-----

From: eNFACT Notifications [mailto:noreply@enfactnotifications.com]

Sent: Thursday, January 26, 2012 11:34 AM

To: Recipients

Subject: eNFACT Case #29018

To protect your account, we monitor your ATM and debit card transactions for potentially fraudulent activity which may include a sudden change in locale (such as when a U.S.-issued card is used unexpectedly overseas), a sudden string of costly purchases, or any pattern associated with new fraud trends around the world.

An eNFACT Case was generated for the cardholder below:

Transaction 1 Information:

A charge on 10/23/2011 in the amount of \$438.09 in ITALY Transaction Score: 981

Transaction 2 Information:

A charge on 10/23/2011 in the amount of \$513.14 in ITALY Transaction Score: 918

Transaction 3 Information:

A charge on 10/22/2011 in the amount of \$0.02 at O RANCH Transaction Score: 37

The eNFACT Case is generated when a suspect transaction is detected. If this transaction was not initiated by you as the credit card holder please follow the steps as shown at : <http://www.efactnotify.com/>

Please be sure to complete the Case Resolution Notification (CRN) Form at (<http://www.efactnotify.com/>) . If you have any questions, or would like additional information pertaining to this eNFACT Case, please contact the Card Processing Center at 800-262-2024.

Please act accordingly now.

If you have received this phishing attack via email, or if you receive it at any time from this point forward:

1. **Do not open** the email;
2. **Do not click** on the link contained in the email; clicking on any of the links contained in the email may install malicious software on your system;
3. **If a link is clicked**, your organization's Information Security personnel should immediately take your system off of the network;
4. **Report** the email to your organization's Information Security personnel;
5. **Delete** the email from your "Inbox" and "Sent Items; and
6. **If you have inadvertently clicked** on the link please notify your local helpdesk for assistance As Soon As Possible.