

**Fraudulent Emails Claiming to be from NACHA
Phishing Alert Update 3/29/2011**



EPCOR and NACHA have received numerous reports this morning that individuals and/or companies are receiving fraudulent emails that have the appearance of being sent from NACHA. Specifically, the email subject line is "ACH Payment Rejected" and appears to be sent from "risk @ nacha.org" See a sample below.

===== Sample Email =====

From: risk@nacha.org [risk @ nacha.org]
Sent: Wednesday, March 30, 2011 7:32 AM
To: Doe, John
Subject: ACH payment rejected

The ACH transaction (ID: 011057709972), recently initiated from your bank account (by you or any other person), was canceled by the Electronic Payments Association.

Please [click here](#) to download report

If you have any questions or comments, contact us at [info @ nacha.org](mailto:info@nacha.org). Thank you for using [http:// www nacha.org](http://www.nacha.org).

=====

The Electronic Payments Association has received reports that individuals and/or companies continue to receive fraudulent emails that have the appearance of having been sent from NACHA. These emails vary in content and appear to be transmitted from email addresses associated with the NACHA domain (@ nacha.org). Some bear the name of fictitious NACHA employees and/or departments.

NACHA itself does not process nor touch the ACH transactions that flow to and from organizations and financial institutions. NACHA does not send communications to persons or organizations about individual ACH transactions that they originate or receive.

- Be aware that phishing emails frequently have attachments and/or links to Web pages that host malicious code and software. Do not open attachments or follow Web links in unsolicited emails from unknown parties or from parties with whom you do not normally communicate, or that appear to be known but are suspicious or otherwise unusual.
- If malicious code is detected or suspected on a computer, consult with a computer security or anti-virus specialist to remove malicious code or re-install a clean image of the computer system.
- Always use anti-virus software and ensure that the virus signatures are automatically updated.
- Ensure that the computer operating systems and common software application security patches are installed and current.

Additional information and guidance on phishing is available from the Federal Deposit Insurance Corporation (FDIC).