Fraudulent Emails Appearing to Come from NACHA

(Updated September 2, 2011)

NACHA, the Electronic Payment Association, 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. Perpetrators are sending these fraudulent messages to email addresses globally.

These fraudulent emails typically make reference to an ACH transfer, payment, or transaction and contain a link or attachment that infects the computer with malicious code when clicked on by the email recipient. The source addresses and contents of these fraudulent emails vary — with more recent examples purporting to come from actual NACHA employees and/or departments — and often including a counterfeit NACHA logo and the citation of NACHA's physical mailing address and telephone number.

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.

As always, you should never 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. Should you receive one of these emails, you are encouraged to forward the suspected fraudulent emails appearing to come from NACHA to abuse@nacha.org to aid in efforts with security experts and law enforcement officials to pursue the perpetrators.

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.