



Tennessee Automated Clearing House Association  
*Tennessee's Electronic Payments Resource*  
[www.nacha.org](http://www.nacha.org)

January 26, 2012

## Fraudulent Emails Appearing to Come from NACHA

### Background

NACHA continues to be 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.

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 contents of these fraudulent emails vary, with more recent examples 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.

Caution your customers not to open attachments or follow Web links in unsolicited emails from unknown parties or from parties with whom they do not normally communicate, or that appear to be known but are suspicious or otherwise unusual. Direct them to forward suspected fraudulent emails appearing to come from NACHA to [abuse@nacha.org](mailto:abuse@nacha.org) to aid in our 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.

### ACTION REQUESTED

NACHA requests that financial institutions, billers, and payment providers ensure that their frontline staff - those who interact with customers - understand the sustained and evolving nature of these attacks. Organizations may wish to consider designating a focal point to coordinate communications and awareness internally and with customers. You can instruct customers to forward fraudulent emails they receive that appear to come from NACHA to [abuse@nacha.org](mailto:abuse@nacha.org) for analysis.

### ADDITIONAL RESOURCES

NACHA has developed a resource page on its website to educate consumers, businesses, financial institutions, and other parties about ways that they can protect themselves from the sustained and evolving phishing attacks in which individuals and organizations in the U.S. and other nations are receiving emails that fraudulently claim to come from NACHA regarding ACH payment transactions. This NACHA resource page can be accessed at: <https://www.nacha.org/Fraud-Phishing-Resources>.

Donna S. Ashworth, AAP  
Executive Director  
Tennessee ACH Association

[Forward this email](#)



This email was sent to swilkerson@volcorp.org by [donna@tacha.org](mailto:donna@tacha.org) | [Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Tennessee ACH Association | 1000 NorthChase Dr., Ste. 201 | Goodlettsville | TN | 37072