



Fraudulent NACHA Email

NACHA has reported that fraudulent emails claiming to be from NACHA are occurring with greater frequency and increased sophistication. 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. The emails and contain a link or attachment that infects the computer with malicious code when clicked on by the recipient. Do not click on any links or open any attachments within the email!

Please Note:

NACHA 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.

Action:

NACHA requests that financial institutions, billers and payment providers ensure that their frontline staff — those who interact with customers/members — 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. If your financial institution, organization and/or your customers receive fraudulent emails that appear to come from NACHA, please forward them to NACHA at abuse@nacha.org for analysis.

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.