

## Examples of Phishing / Fraudulent Emails

Millions of fraudulent emails are sent and circulated daily. Fraudulent emails claim to come from a wide variety of sources including NACHA (National Automated Clearing House Association). These emails are known as phishing emails and the fraudsters sending them are known as phishers.

At NACHA, we take security and the risk posed by these phishing campaigns very seriously. We monitor phishing activity regularly and initiate takedown of fraudulent (malware) websites as soon as they are reported or we are made aware of them. Our members are valuable partners in reporting and helping prevent fraud. A knowledgeable consumer or business can also prevent fraud by understanding how to spot fraudulent emails and staying up to date on general computer, internet, mobile, and email security tips.

The emails below are provided solely to give you an idea of what fraudulent emails may look like. NACHA did not send them, and our systems have not been compromised in any way.

NACHA does not process nor otherwise touch the ACH transactions that flow via the [ACH Network](#) nor between financial institutions and their customers.

NACHA does not send communications of any type to persons or organizations about individual ACH transactions that they originate or receive. If you or your customer has received a communication of this nature that purports to come from NACHA, it is fraudulent.

You may have received a fraudulent email that differs from these examples.

## Examples of Recent Fraudulent Emails Include

### Fraudulent Email Example 1

*(subject lines vary, random number generation, cancelled, rejected, denied)*

Subject: ACH Payment 3396043 Cancelled

Payment Notification # 3356941

The ACH Transaction (ID:33456941), recently initiated from your checking account (by you or another person) was cancelled by the other financial institution.

**Rejected transaction ID:33456941**

**Reason for Rejection: See details in the attachment.**

**Transaction Report: report\_3482735.pdf.zip Winzip archive, pdf document**

### Fraudulent Email Example 2

*(subject lines vary, at random-reputable company name and payment amount inserted)*

Subject: Pending Payment request from "reputable company name inserted here"

We recorded a payment request from "reputable company name inserted here" to enable the charge of \$170.10 on your account.

Receipt number: 45287954

The payment is pending for the moment.

If you made this transaction or if you just authorize this payment, please ignore or remove email message.

The transaction will be shown on your monthly statement as "reputable company name inserted here"

If you didn't make this payment and would like to decline it, please click on the link below:

[Decline transaction #40683343 from "reputable company name inserted here": \\$170.10](#)

Best regards, "reputable company name inserted here"

### Fraudulent Email Example 3

*(subject lines vary)*

Subject: ACH Transfer Review

Dear Client,

ACH Transfer (ID:03847439) is going to be reviewed because of the incorrectly input data when sending the payment.

**Important: Please fill in the application form attached attentively and send it to us. After that your transfer will be processed.**

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

Employee Name

Risk Management Services