Consumer Alerts

Reports of suspicious or fraudulent activity involving banking consumers or products. Receive email updates on these issues by subscribing to Consumer Alerts.

E-mail Claiming to Be From the FDIC – January 30, 2013

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports of fraudulent e-mails that have the appearance of being sent from the FDIC.

While the e-mails exhibit variations in the "From" and "Subject" lines, the messages are similar.

The fraudulent e-mails are addressed to the attention of the “Accounting Department” and meant to notify recipients that that that “ACH and WIRE transactions” are being blocked until “a special security software” is installed.

They then instruct recipients to go to a Web site for instructions on how to download the necessary files by clicking on a hyper-link provided (Note: the Web site addresses (URL) vary widely).

This e-mail and link are fraudulent. Recipients should consider the intent of this e-mail as an attempt to collect personal or confidential information, or to load malicious software onto end users' computers. Recipients should not click on the link provided.

The FDIC does not issue unsolicited e-mails to consumers or business account holders.

Fraudulent E-mails Claiming to Be From the FDIC - October 3, 2012

This message is to notify you of fraudulent e-mails in circulation claiming to be from the FDIC. Please consider both to be fraudulent.

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports of fraudulent e-mails that have the appearance of being sent from the FDIC.

While the e-mails exhibit variations in the "Subject" lines, the messages are similar. They all make reference to the suspension of recipient’s ability to conduct transfers via ACH and/or wire transfer. The e-mails then encourage recipients to install a software update by clicking on a link provided. They then say that functionality will be restored once the software update is installed.

These e-mails and the link provided are fraudulent. Recipients should consider the intent of these e-mails to load malicious software on the recipient’s computer, or to collect personal or confidential information. Recipients should not click on the link provided.

The FDIC does not send unsolicited e-mails to consumers or business account holders.

Fraudulent E-mails in Circulation – September 13, 2012

This message is to notify you of two fraudulent e-mails in circulation claiming to be from the FDIC. Please consider both to be fraudulent.

The first fraudulent email includes statements pertaining to the Bankruptcy Reform Act of 1978 and the Investor Protection Law under the Securities Act of 1933. The contact information claims to be fdic.gov@execs.com, and the area code of (646) is used is for the Washington Office. The FDIC does not have email addresses @execs.com and (202) is the area code for the Washington Office. A form, which is attached to the cover letter, purports to be an "FDIC Claimant Verification" form. It

too is fraudulent.

The second fraudulent email claims to originate at support@fdic.gov and pertains to ACH transactions. The recipient is told that an ACH transaction has not been delivered; the recipient is requested to download the update via a link.

These e-mails are fraudulent and were not sent by the FDIC. Recipients should consider these e-mails as an attempt to steal money or obtain personal or confidential information from the recipient. Recipients should NOT, under any circumstances, send funds as requested or provide any personal financial information. Also, please do not click on the links provided in the fraudulent emails, as this may load malicious software onto end users' computers. As a reminder, the FDIC does not send unsolicited emails to consumers or business account holders.

Fraudulent E-mail Survey – April 27, 2012

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports of fraudulent e-mails that have the appearance of being sent from the FDIC.

The e-mail exhibits the "Subject" line: "SURVEY CODE: STJSPNUPUT". The "From" line may exhibit variations; however, the messages are similar.

The email states, "You have been chosen by the FDIC to take part in our quick and easy 5 questions survey. In return we will credit $100 to your account just for your time!" The recipient is then instructed to "Click here to Continue." **Recipients should not click on the link provided.**

This email and link are fraudulent. Recipients should consider the intent of the email as an attempt to collect personal or confidential information, or to load malicious software onto end users' computers. As a reminder, the FDIC does not send unsolicited emails to consumers or business account holders.

Previous Alerts

- Consumer Alerts - 2012
- Consumer Alerts - 2011
- Consumer Alerts - 2010

Last Updated 1/30/2013

Customer Assistance Online Form

Below are examples of fraudulent e-mails reported to fraud@ups.com and presented here in an effort to inform and educate businesses and consumers of fraudulent activities. Some e-mails or attachments may contain viruses.
*NOTE: Images or logos sometimes included are not shown in these examples.

From: UPS [mailto:admindept@ups.com]
Sent:
To:
Subject: UPS Tracking Number H5825718929

Various return addresses are used.

You can use UPS TEAM to:

- Ship Online
- Schedule a Pickup
- Open a Your UPS CUSTOMER SERVICES Account

Welcome to UPS TEAM

May also say "Welcome to UPS Customer Services".

Good afternoon!, **Cmunchak**.

DEAR USER , RECIPIENT'S ADDRESS IS WRONG

Please fill in attached file with right address and resend to your personal manager.

With Respect To You , Your UPS .COM.

Do not open any attachments or click on any links.

Copyright 2011 United Parcel Service of America, Inc. USPS .us Customer Services, the Your USPS .us Customer Services brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.

Please do not reply directly to this e-mail. USPS Team will not receive any reply message. For questions or comments, visit Contact UPS.

We understand the importance of privacy to our customers. For more information, please consult the Your USPS Team Privacy Policy.

This communication contains proprietary information and may be confidential If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.

Below are examples of fraudulent e-mails reported to fraud@ups.com and presented here in an effort to inform and educate businesses and consumers of fraudulent activities. Some e-mails or attachments may contain viruses.
*NOTE: Images or logos sometimes included are not shown in these examples.

From: "UPS Express Services" <identification@ups-us.com>
Date: August 15, 2012 5:23:12 PM EDT
To: [redacted]
Subject: Delivery information # Error ID7384
Reply-To: "UPS Express Services" <identification@ups-us.com>

Various return addresses and may have domain @ups-usa.com or @upsus.com.

Subject may be Status ID, Refuse ID, or similar wording.

WE ♡ LOGISTICS™

Unfortunately we failed to deliver the postal package you have sent on the 27th of July in time, because the recipient's address is erroneous.

Please print out the label copy attached and collect the package at our office.

Print a shipping Label

Below are examples of fraudulent e-mails reported to fraud@ups.com and presented here in an effort to inform and educate businesses and consumers of fraudulent activities. Some e-mails or attachments may contain viruses.
*NOTE: Images or logos sometimes included are not shown in these examples.

From: Lester Otto [mailto:USPS Shipping Services@usps.com]
Sent: Tuesday, July 10, 2012 12:04 PM
Subject: You have new UPS invoices.

This is an automatically generated email Please do not reply to this email address.

Valued UPS Customer,

New invoice(invoices) are available for download in UPS billing center. Do not forget that your UPS invoices should be paid within 28 days to avoid any additional charges.

Please visit the UPS Billing Center to download and pay your invoice.

Hold cursor over hyperlink to reveal deceptive link, not a valid UPS link

Find out more about UPS:
Visit ups.com
Explore UPS Freight Services
Learn About UPS Companies
Sign Up For Additional Email From UPS
Read our official blog

(c) 2012 United Parcel Service of America, Inc. UPS, the UPS brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.
For more information on UPS's privacy practices, refer to the UPS Privacy Policy.
Please do not reply directly to this e-mail. UPS will not receive any reply message.
For questions or comments, visit Contact UPS.

This communication contains proprietary information and may be confidential. If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.
Privacy Policy
Contact UPS

SHARE

Examples of Phishing / Fraudulent Emails

Millions of fraudulent emails are sent and circulated daily. Fraudulent emails claim to come from a wide variety of legitimate entities, including NACHA. 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 Fraudulent Emails

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. Thank you for using www.nacha.org.

Employee Name

Risk Management Services