



# MEMBERS MEMO

*A periodic update of significant NACHA projects, programs and information*



## THE NACHA MEMBERS MEMO

*For distribution to Participating Depository Financial Institution members*

March 14, 2007

### Fraud Scenarios – Reverse Phishing and Keylogging

This edition of the NACHA Members Memo provides information about two scenarios that have resulted in fraud losses.

#### **CASE 1 - CORPORATE “REVERSE PHISHING”**

The following fraud scenario has been reported to NACHA. NACHA is calling it a case of “reverse phishing”; instead of e-mails attempting to fraudulently obtain corporate banking information, the perpetrator(s) sent e-mails fraudulently providing corporate banking information.

#### *The scenario:*

- A company received e-mails from two trading partners asking for changes to bank and account numbers used to receive ACH payments for invoices;
- The company believed the requests to be legitimate, as the e-mails looked like those from the trading partners;
- The company originated ACH credits to the new bank and account numbers for these trading partners;
- The ACH credits went to newly opened accounts, and the funds were withdrawn;
- Eventually, the company received phone calls from the trading partners about failure to pay;
- The company investigated and discovered that the original e-mails supplying new payment instructions were fraudulent.

#### *Recommendations:*

- Originators should perform due diligence in accepting changes in payment instructions. For example, a widely used security procedure is a callback to a known individual at the trading partner.
- ODFIs can alert their Originators to this type of fraud scheme.

## **CASE 2 - KEYLOGGING SPYWARE**

The following fraud scenario has been reported to NACHA by several parties, and resulted in bank losses. The scenario takes advantage of compromised IT security, poor corporate treasury management practices, and weak authentication. The scenario is not specific to ACH payments; wire transfers were involved as well.

### ***The scenario:***

- A corporate treasury workstation or computer used to log on to online banking is infected with keylogging spyware;
- The keylogging spyware records the company's online banking credentials - User ID and Password – when an employee signs in to online banking;
- The keylogging spyware then sends this information to the perpetrator;
- The perpetrator uses the company's credentials to sign in to online banking on the corporate banking web site;
- The perpetrator initiates outbound funds transfers out of the company's corporate account(s), either via ACH credits or wire transfers
- The company does not employ any additional means to confirm the transactions and release funds, and the bank does not require additional authentication of the party initiating the transfers;
- The perpetrator routes funds to deposit accounts at various financial institutions; these accounts were recently opened either by the perpetrator, or arranged to be opened through willing associates or unknowing individuals;
- These accounts receive deposited good funds via ACH credits or wire transfers;
- The account owners then wire funds overseas, and are non-recoverable by the company and its bank.

### ***Recommendations:***

#### **Originators**

- Originators should use best practices for treasury management and corporate banking, including authentication for authorizing transactions online and/or independent confirmation of outbound transfers;
- Originators should reconcile their accounts daily;
- Originators should use best practices for information technology security, covering the integrity of hardware, software and identity management.

#### **ODFIs**

- ODFIs should use best practices for authenticating corporate customers and executing instructions for outbound funds transfers initiated online;
- ODFIs should work with their Originators on best practices for corporate banking and IT security;
- ODFIs can alert their Originators to this type of fraud scheme.

## **TERMS OF USE**

Payment Associations may distribute this NACHA Members Memo to their Participating Depository Financial Institution members. Due to the nature of these fraud schemes, Participating DFI members may distribute this NACHA Members Memo to their Originators that would find it of interest.

## **IMPORTANT DATES**

March 16, 2007 – Back Office Conversion becomes effective.

March 21, 2007 – Teleseminar: Cross-Channel Risk and Third Party Access. See [http://www.nacha.org/conferences/teleseminars/Tele\\_3rdPartyAccess/Tele\\_3rdPartyAccess.htm](http://www.nacha.org/conferences/teleseminars/Tele_3rdPartyAccess/Tele_3rdPartyAccess.htm).

April 15-18, 2007 – PAYMENTS 2007, Chicago, Illinois. See <http://www.nacha.org/conferences/Payments2007/default.htm>.

April 23, 2007 – Comments due on the Network Enforcement Proposal. See [http://www.nacha.org/ACH\\_Rules/Rule\\_Making\\_Process/Rules\\_Work\\_Groups/RFC-022007/default.htm](http://www.nacha.org/ACH_Rules/Rule_Making_Process/Rules_Work_Groups/RFC-022007/default.htm).

May 2007 – National Direct Deposit and Direct Payment Month. See <http://www.electronicpayments.org>.

May 1-2, 2007 – Global Payments Forum meeting. See <http://gpf.nacha.org/MeetingNoticeMay2007/meetingnoticemay2007.htm>.

May 17, 2007 – Teleseminar: Walk-In Payments: Best Practices and Emerging Trends. See [http://www.nacha.org/conferences/teleseminars/Tele\\_WalkInPmts/Tele\\_WalkInPmts.htm](http://www.nacha.org/conferences/teleseminars/Tele_WalkInPmts/Tele_WalkInPmts.htm).

May 21-22, 2007 – Council for Electronic Billing and Payment meeting, San Antonio, Texas. See <http://cebp.nacha.org/>.

May 21-22, 2007 – Electronic Check Council meeting, San Antonio, Texas. See <http://ecc.nacha.org/>.

May 22-24, 2007 – EBS Council meeting, Baltimore, Maryland. See <http://ebt.nacha.org/ebt-meetinginfo/ebt-meetinginfo.html>.

May 23-24, 2007 – Corporate Payments Council meeting, San Antonio, Texas. See [http://www.nacha.org/corporate\\_payments/Meetings/May2007Notice/may2007notice.htm](http://www.nacha.org/corporate_payments/Meetings/May2007Notice/may2007notice.htm)

May 23-24, 2007 – Internet Council meeting, San Antonio, Texas. See <http://internetcouncil.nacha.org/>.

####