OCC ALERT

Comptroller of the Currency
Administrator of National Banks

Subject: Customer Identity Theft: E-Mail-Related Fraud Threats

TO: Chief Executive Officers and Chief Information Technology Officers of National Banks, Federal Branches, Service Providers, Department and Division Heads, and Examining Personnel

PURPOSE

This alert is intended to raise awareness of an increasingly common Internet fraud called "phishing" and encourages banks to educate their customers, strengthen monitoring systems, and enhance response programs to reduce the potential risk to their organizations and customers.[1]

BACKGROUND

The FBI's Internet Fraud Complaint Center (IFCC) reports a steady increase in complaints involving unsolicited e-mails directing consumers to a phony "customer service" Web site or directly asking for customer information. These scams are contributing to a rise in identity theft, credit card fraud, and other Internet-based frauds.[2] E-commerce customers, including bank customers, have fallen victim to these scams.

Phishing involves sending customers a seemingly legitimate e-mail request for account information, often under the guise of asking the customer to verify or reconfirm confidential personal information such as account numbers, social security numbers, passwords, and other sensitive information. In the e-mail, the perpetrator uses various means to convince customers that they are receiving a legitimate message from someone whom the customer may already be doing business with, such as a bank. Techniques such as a false "from" address or the use of seemingly legitimate bank logos, Web links, and graphics may be employed to mislead the customer. After gaining the customer's trust, the perpetrator attempts to convince the customer to provide personal information and provides one or more methods for the customer to communicate that information back. For example, the e-mail might include a link to the perpetrator's Web site that contains a form for entering personal information. Like the e-mail, the Web site is designed to trick the customer into believing it belongs to the bank. Alternatively, the e-mail might simply include an embedded form for the customer to complete. The ultimate goal of this fraud is to use the customer information to gain unauthorized access to a customer's bank or financial accounts or to engage in other illegal acts.

[1] Refer to the FFIEC Information Technology Examination Handbook's "Information Security Booklet" located at www.ffiec.gov.
[2] Federal Bureau of Investigation Press Release, "FBI Says Web 'Spoofing' Scams are a Growing Problem", July 21, 2003.

RISK MITIGATION FOR E-MAIL-RELATED FRAUDS

Banks should implement appropriate controls consistent with the security process described in the Federal Financial Institutions Examination Council's (FFIEC) "Information Security Booklet." Management should consider the following actions to help prevent, detect, and respond to the threat from e-mail-related frauds:

Prevention

- Provide notices on Web sites reminding customers that the bank will never request confidential information through e-mail and to report any such requests to the bank.
- Print warnings and notices on customer statements or other paper mailings.
- Improve authentication methods and procedures to protect against the risk of user ID and password theft from the customer through e-mail and other frauds. Authentication methods solely reliant on shared secrets (e.g., passwords) are more susceptible to phishing schemes than stronger authentication methods.[3]
- Review and, if necessary, enhance practices for protecting confidential customer data.
- Maintain current Web site certificates and describe how the customer can authenticate the bank's Web pages by checking the properties on a secure Web page.
- Refer customers to or use Federal Trade Commission (FTC) resources to develop educational brochures to explain the red flags and risks of identity theft.
  - FTC, "How Not to Get Hooked by the 'Phishing' Scam," July 2003 http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
  - FTC, "ID Theft: When Bad Things Happen to Your Good Name," September 2002 http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Detection

- Monitor accounts individually or in aggregate for unusual account activity such as address or phone number changes, large or a high volume of transfers, and unusual customer service requests.
- Monitor for fraudulent Web sites using variations of the bank's name.[4]
- Establish a toll-free number for customers to verify requests for confidential information or to report suspicious e-mails.
- Train customer service staff to refer customer concerns regarding suspicious e-mail request activity to security staff.

Response

- Incorporate notification of known e-mail-related frauds into the response program to alert customers of fraudulent requests for information and to caution them against responding.
- Establish a process to notify Internet service providers, domain name issuing companies, and law enforcement to shut down fraudulent Web sites and other Internet resources that are being used to facilitate phishing or other fraudulent e-mail practices.
- Increase suspicious activity monitoring and employ additional identity verification controls.
- If fraud is detected in connection with customer accounts, the bank should report the fraud and consider offering its customers assistance consistent with the comprehensive guidance on

[3] Refer to OCC Advisory Letter 2001-8, "Authentication in an E-Banking Environment."
[4] Refer to OCC Alert 2000-9, "Protecting Internet Addresses of National Banks."

reporting and customer assistance given in OCC Advisory Letter 2001-4, "Identity Theft and Pretext Calling."

In the event your institution is a victim of an e-mail-related scam, you should promptly notify your OCC supervisory office. As appropriate, you should also report the event to law enforcement by filing a Suspicious Activity Report.

Questions regarding this alert should be directed to Clifford A. Wilke, director for Bank Technology Policy at (202) 874-5920 or clifford.wilke@occ.treas.gov.

_____

Ralph E. Sharpe
Deputy Comptroller for Technology