

FDIC - Identity Theft Symposium: Fighting Back against Phishing and Account Hijacking

February 11, 2005

AED Conference Center
1825 Connecticut Ave., NW, 8th Floor
Washington, DC 20009
(202) 884-8600

10:30 AM What More Can Be Done to Fight Phishing: The Industry Perspective

Moderator: Michael Jackson, Associate Director, Division of Supervision and Consumer Protection, FDIC

Panelists:

- American Bankers Association , Wayne Abernathy, Executive Director
- Michael J. Curcio, Executive Vice President, E*TRADE Securities
- Brian Kennedy, Vice President, Fraud Policy, Citicards North America

Background:

The FDIC issued FDIC FIL-132-2004 "Putting an End to Account-Hijacking Identity Theft, December 14, 2004. Comments are due to FDIC via email no later than Friday, February 11, 2005.

The ABA is tasked with developing a position on the issues raised by the FDIC study and respond to FDIC with a comment letter.

The FDIC Study focuses on the specific problem of "account hijacking," and is presented as a subset of the larger problem of "identity theft." This allows FDIC and banks to focus on a specific set of threats and potential counter-measures without having to address the broader realm of "identity theft" issues. FDIC defines account hijacking as "unauthorized access to and misuse of existing asset accounts."

The FDIC Study contends that account hijacking is largely a consequence of (1.) reliance on single-factor authentication for customers accessing financial services, and (2) lack of authentication for communications from banks to their customers. FDIC contends that "Phishing" and "hacking" are the primary threats leading to hijacking accounts, and that "account hijacking is the fastest growing form of identity theft."

The FDIC Study suggests four steps that the financial industry might take to reduce this form of online fraud:

1. Adopt two-factor authentication for customer access to financial services.
2. Employ “scanning software” to detect and defend against Phishing attacks.
3. Strengthen customer education programs.
4. Promote information sharing between financial institutions, government agencies and technology providers.

It is the first of these four suggestions that require our attention, as the other three are already being implemented by most, if not all, ABA members involved in online banking.

Proposed Position:

The ABA commends the FDIC for focusing attention on this issue. There are many means of achieving greater security in online financial transactions. Two-factor authentication is one of these means, and may be appropriate for certain applications. We must consider though, that deploying such a solution will require considerable cross-industry cooperation. Such cooperative efforts as the Electronic Authentication Partnership (EAP) are working toward establishing commonly accepted levels of assurance, liability and taxonomy. Other considerations such as cost of deployment, consumer acceptance and ease of use must be addressed. Authentication methods must be appropriate for their intended uses, must be acceptable to consumers and be cost-effective. The ABA encourages industry initiatives to improve online authentication practices. The challenge of “mutual authentication” must be addressed in a manner so that every customer is able to trust communications from their banks while having the confidence that their account will not be “hijacked” by fraudulent actors on the Internet. The financial industry has so far been able to largely contain the threat from fraudsters. The real threat to financial institutions is the threat to trust and confidence in the online channel. Banks as well as regulators can both play a role in countering the threat to this trust and confidence.

The ABA strongly encourages the FDIC, other regulatory agencies and financial institutions to:

1. Encourage the industry to adopt stronger online authentication, and to deploy solutions appropriate to the risk at each level of assurance. Two-factor authentication is one means of stronger online authentication, and may be appropriate for some levels of assurance. Other means are also commercially available and should be considered for deployment according to the risk presented.
2. Promote industry standards for assurance, liability and taxonomy for establishing identity and stronger online authentication.
3. Strengthen customer education programs.

4. Promote information sharing between financial institutions, government agencies and technology providers.

ABA Anti-Phishing Initiatives

1. The ABA is presently working to set up an ABA Anti-Phishing website. Anticipated completion date: 1st Quarter 05

2. The ABA has taken the lead in an effort to coordinate anti-Phishing efforts with the International Banking Federation (IBFED), which includes the British Bankers Association, APACS (Association for Payment Clearing Services), the Australian Bankers Association, and the European Banking Federation. This will include establishing points of contact, definitions/taxonomy, information sharing channels (ABA and APACS already sharing information) and joint public relations as well as consumer and banker education. APACS currently produces an anti-Phishing website “Banksafeonline.” (Link noted below)

3. A series of anti-Phishing, electronic fraud and privacy sessions to held at the upcoming ABA Technology, Community Bankers, and Compliance Conferences in 2005.

4. A webcast for ABA members titled “Protecting your Customers” is scheduled for April 2005.

5. The ABA is participating in anti-Phishing initiatives with other associations, such as The Financial Services Technology Consortium (FSTC)’s Counter-Phishing Project (Phase 1 complete; NACHA’s Internet Council’s Financial Institution Authentication Working Group and BITS Security and Risk Assessment Working Group.

6. The ABA is a participant in the GSA sponsored “Electronic Authentication Partnership” (EAP). The EAP is a multi-industry partnership working on the vital task of enabling interoperability among public and private electronic authentication (e-authentication) systems.

7. The ABA is an equity partner in Identrus, LLC. Identrus helps organizations surmount the final obstacle preventing business-to-business Internet commerce from thriving: authentication of identity using digital certificates within a Public Key Infrastructure (PKI).

8. ABA Communications has produced an Identity Theft Communications Kit, an Identity Theft Speech for bankers, talking points and statement stuffers available for members.

References:

FDIC FIL-132-2004 "Putting an End to Account-Hijacking Identity Theft"
(comments due to FDIC via email 2/11/05)

<http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html>

FSTC Counter-Phishing Project- Phase 1 Whitepaper and supporting documents

<http://fstc.org/projects/counter-phishing-phase-1/>

The Electronic Authentication Partnership

<http://www.eapartnership.org/>

APACS Anti-Phishing webpage

<http://www.banksafeonline.org.uk/>

Identrus, LLC

www.Identrus.com