

# *WHO IS ON THE OTHER END OF THE LINE?*

## *Authentication for E-Banking*



*George Mori  
Operations Risk Coordinator  
Federal Reserve Bank of San Francisco  
[George.mori@sf.frb.org](mailto:George.mori@sf.frb.org)*

# Agenda

- Introduction (3 - 9)
- Assessing risk and controls (10 - 16)
- Customer awareness (17 – 19)
- Questions (20)

*The following presentation contains the views and opinions of the speaker and his interpretation of regulatory guidance, and does not necessarily reflect the views of the management of the Federal Reserve Bank of San Francisco or the Board of Governors.*

# *Introduction*

From: SecurityDepartment@anybank.com  
Subject: AnyBank Anti-Fraud Verification Procedure  
Date: 16 Aug 2006 14:16:36

**Dear AnyBank.com Customer,**

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:

[http://www.anybank.com/personal/Checking/OnlineBanking/Internet\\_Banking/index\\_bhcp=3d1](http://www.anybank.com/personal/Checking/OnlineBanking/Internet_Banking/index_bhcp=3d1)

Note: Requests for information will be initiated by AnyBank Business Development; this process cannot be externally requested through Customer Support.

Sincerely,  
AnyBank  
Security Department.

Dear OtherBank customer,

OtherBank is committed to maintaining a safe environment for its community of buyers and sellers. Protecting the security of your account and of the OtherBank network is our primary concern. In this respect, as a preventative measure, we have recently revised your account information data in order to assure ourselves that the most advanced security techniques in the world and our anti-fraud teams regularly screen the OtherBank system for any unusual activity. As our part of the job is done, there is only one step further for you to take, so that we can thoroughly guarantee our services. Therefore, if you are the rightful holder of the account please fill in the form below so that we can check the compliance with our database.

<https://onlinebanking.otherbank.com/OnlineBanking/login.aspx?ReturnUrl=%2fOnlineBanking%Default.aspx>

If you believe you have provided personal or account information in response to a fraudulent e-mail or Web site, please contact OtherBank at (555) 555-1212 and contact the other financial institutions with which you have accounts.

Thank you for trusting our services.

Sincerely,  
The OtherBank Security Department Team,

Thank you for your prompt attention to this matter.  
OtherBank - Fraud Center

## **Aust(-ralian) Trojan teens arrested over Internet bank scam**

Munir Kotadia, ZDNet Australia  
January 06, 2005

At least four Australian teenagers have been arrested for their alleged part in an Internet banking scam that has generated millions of dollars..... the two boys and two girls, aged between 16 and 17, were allegedly used as "mules" by organized criminals. ....

Nine more suspects have been arrested including two men, aged 19 and 21, who are allegedly thought to be ringleaders of the international crime gang's Australian operation.

According to the NSW Police, the gang used adverts and spam to distribute malware that, once loaded on a computer, could monitor the user's keystrokes and send any banking usernames and passwords back to the gang's ringleaders.

# *Why Amend Regulatory Expectations?*

- Change in legal requirements
- Advances in technology
- Criminal application of technology
- Increased media attention

# *Why Should Bankers Care If The Customer Is Tricked?*

## ➤ Reputational risk

- Customer faith in integrity of bank controls

## ➤ Legal / regulatory risk

- Responsibility to maintain prudent controls
- GLBA 501(b)

# *Who Does The Guidance Apply To?*

- Interagency guidance
- All financial institutions
- Deadline for conformance yearend 2006

# *Assessing Risks and Controls*

# *Defining Terms*

- Customer
- High risk transactions:
  - Confidential customer information
  - Transfer of funds
- Types of preventative controls for multifactor authentication:
  - Something the customer knows
  - Something the customer has
  - Something the customer is

# *Understanding Inherent Risk*

- Types of high risk services
- Volume / size of transactions
- Types of customers

# *Identifying Threats*

- Unauthorized access to:
  - Confidential customer information
  - Funds transfer features
- How do they accomplish this:
  - Social engineering / Phishing
  - Pharming
  - Malware

# *Assessing Controls*

## Preventive Controls:

- Single factor authentication
- Multi-factor authentication
- Mutual authentication
- Other controls

# *Assessing Controls*

## *(continued)*

- **Detective controls:**
  - Audit logs
  - Timely and regular review of logs
- **Corrective controls (incident response plan)**
- **Documentation**
- **Vendor risk assessment**

# *Addressing The Risk Exposure*

- Identify services requiring stronger controls
- Develop/Document/Execute detailed project plan
- Information security standards

# *Customer Awareness*

## Citibank Phish Spoofs 2-Factor Authentication

WashingtonPost.com

July 10, 2006

Brian Krebs

“a Web-based e-mail that targets users of **Citibank's Citibusiness** service...

The scam e-mail says someone (a nice touch added here -- the **IP address** of the imaginary suspect) has tried to log in to your account and that you need to "confirm" your account information. ...when you click on the link, you get a very convincing site that looks identical to the Citibusiness login page, complete with a longish Web address that at first glance appears to end in "Citibank.com," but in fact ends at a Web site in Russia called "**Tufel-Club.ru.**"

The site asks for your user name and password, as well as the token-generated key. If you visit the site and enter bogus information to test whether the site is legit you might be fooled. That's because this site acts as the "man in the middle" -- it submits data provided by the user to the actual Citibusiness login site. If that data generates an error, so does the phishing site, thus making it look more real.”

# *Customer Awareness Program*

- Key defense
- Customer awareness education
- Periodically update program
- Consider metrics to measure effectiveness

# *QUESTIONS*