AuditLink

FFIEC Guidance and Supplement to Authentication in an Internet Banking Environment

Jim Vilker, NCCO

VP of Professional Services, CMS

Audit Link, A Division of CU*Answers

Patrick Sickels, CISA

Internal Auditor, CU*Answers

November 2, 2011

Agenda

- Review FFIEC Supplement
- Review CU*Answers Guidance
- Review CU*Answers Position Paper
- Moving forward

Why?

- Losses and law suits relative to account take overs are on the rise
  - Sophistication of hacking techniques
  - Organized cyber crime targeting financial institutions
  - Authentication mechanisms and security controls are being compromised

Why?

FBI Investigating Over 400 Corporate Account Takeovers

Friday, September 16, 2011

The Federal Bureau of Investigation's assistant director of the Cyber Security Division, Gordon M. Snow, presented Congressional testimony this week on the ever growing impact of cyber crime on American businesses and consumers.

Snow presented his statements to a House Financial Services subcommittee governing financial institutions and consumer credit issues.

Snow revealed that the FBI is currently investigating a surprisingly large number of corporate banking account breaches, with losses from ACH fraud and bogus wire transfers in the tens-of-millions of dollars.

"The FBI is currently investigating over 400 reported cases of corporate account takeovers in which cyber criminals have initiated unauthorized ACH and wire transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of over $255 million and have resulted in the actual loss of approximately $85 million," Snow testified.

AuditLink

Why?

N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss

European Cyber-Gangs Target Small U.S. Firms, Group Says

e-Banking Bandits Stole $465,000 From Calif. Escrow Firm

La. firm sues [bank] after losing thousands in online bank fraud

Cyber attackers empty business accounts in minutes

Zeus hackers could steal corporate secrets too

TEXAS FIRM BLAMES BANK FOR $50,000 CYBER HEIST

Computer Crooks Steal $100,000 from Ill. Town

FBI Investigating Theft of $500,000 from NY School District

Zeus Botnet Thriving Despite Arrests in the US, UK

NCUA Expectations

"Federally insured credit unions will be expected to adapt appropriate strategies from the supplement to strengthen and enhance controls by January 2012. Beginning in 2012, at credit unions offering electronic services, NCUA examiners will evaluate these controls under the enhanced expectations outlined in the supplement"

Debbie Matz
Chairman, NCUA

http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf

http://www.ncua.gov/Resources/Pages/LCU2011-09.aspx

FFIEC Supplement

Risk Assessment Frequency

- As new information becomes available
- Prior to implementing new electronic services
- Or, at least every twelve months

FFIEC Supplement

Risk Assessment Considerations

- Changes in the internal and external threat environment, including those discussed in the Appendix to this Supplement;
- Changes in the customer base adopting electronic banking;
- Changes in the customer functionality offered through electronic banking; and
- Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

FFIEC Supplement

What Transactions are Covered

Remains unchanged from the original 2005 guidance and is defined as:

Electronic transactions involving access to customer information or the movement of funds to other parties. Not every on line transaction poses the same amount of risk. More controls should be added as the risk level increases.

- In itsme247
  - Transfers to other members accounts
  - Bill Pay
  - A2A

FFIEC Supplement

Retail vs. Business Commercial Banking

- Retail poses comparatively lower risk as the frequency and dollar amount or lower
  - *Implement layered security for those accounts consistent with the risk*
- Business transactions generally involve ACH file origination and frequent interbank wire transfers
  - *Implement layered security for those accounts consistent with the risk*
  - *Offer multi factor authentication*

FFIEC Supplement

Layered Security Programs

- Use of fraud detection systems
- Dual customer authorization
- Use of out-of-band verification
- Thresholds
- IP blocks
- Control over account maintenance activities
- Customer education

AuditLink

Position Paper

"We are ready if you are"

1. Conduct Risk Assessment
2. Identify high risk transactional commercial accounts and set PIB
3. Identify other high risk transactional accounts and set up layered security
4. Monitor and set controls for accounts
5. Provide member education

Step One - Risk Assessment

Risk Assessment Frequency

- As new information becomes available
- Prior to implementing new electronic services
- Or, at least every twelve months

Risk Assessment Considerations

- Changes in the internal and external threat environment, including those discussed in the Appendix to this Supplement;
- Changes in the customer base adopting electronic banking;
- Changes in the customer functionality offered through electronic banking; and
- Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

Step One - Risk Assessment

- Go to: http://cuanswers.com/security/index.php
- Document the features you currently have turned on and rate the level of risk associated with each one. Concentrate on those where money is transferred out of the member account
- Document controls you have activated
  - Password retries
  - Maximum withdrawals
  - PIB
  - Account opening procedures to identify high risk accounts

Step One - Risk Assessment

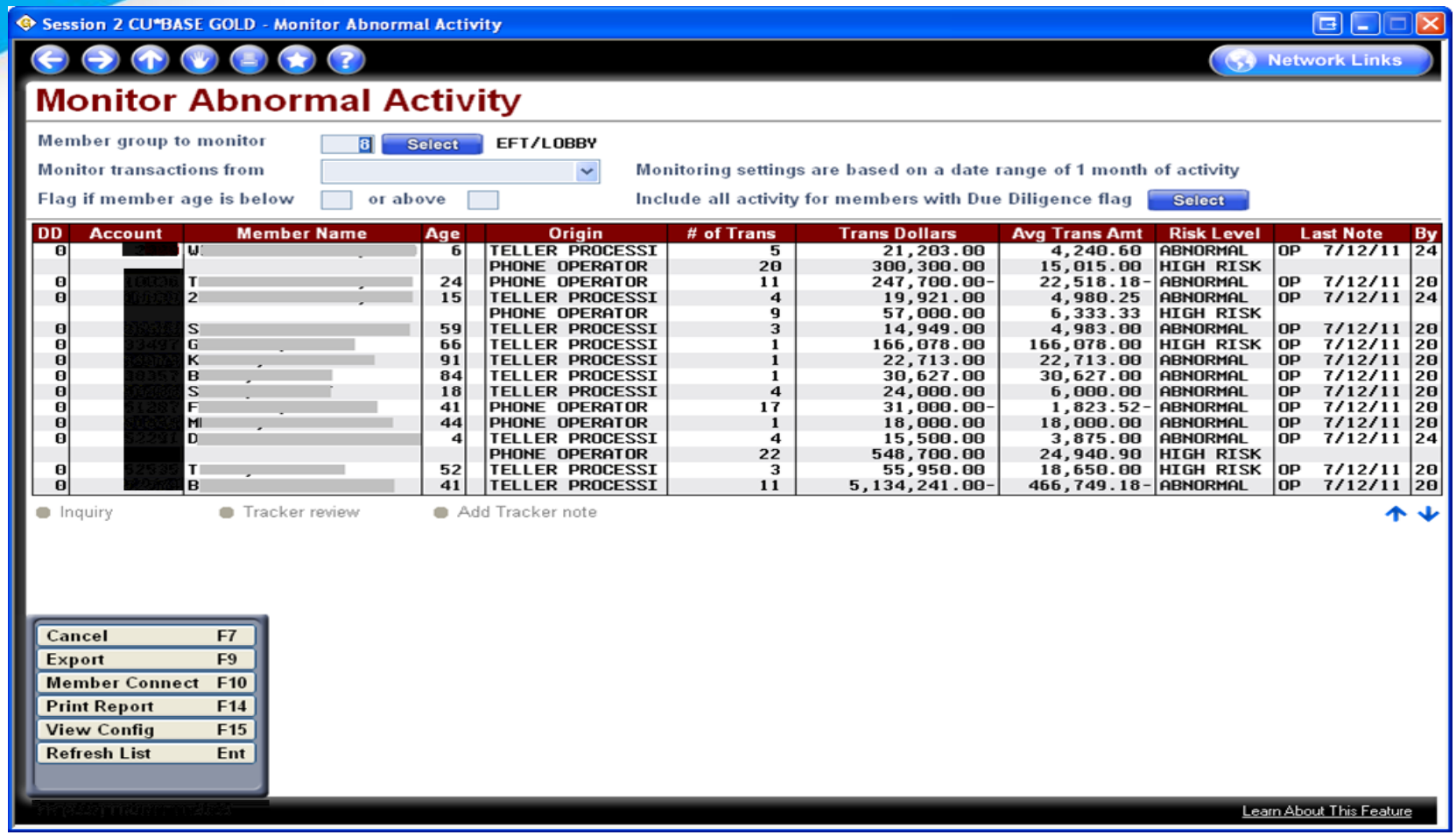
- Document the type of member accounts you currently support, field of membership characteristics, and rate them relative to overall risk (much like your OFAC assessment)
- Determine the level of risk and document the appropriate changes required in processing new accounts, identifying existing high risk accounts, and monitoring them for suspicious activity
- Based upon the above formalize a statement as to the overall risk the credit union has and formalize the assessment for the Board of Directors.

What's Next

- Additional CU*BASE Analytics (spring 2012)
  - Establishing high risk tests based upon member designation for normal, abnormal, and high risk accounts
  - Runs can be done on any timeframe not just end of month and be based upon transaction volume and/or dollar amount
  - Ability to multiple origins (cross channel)
  - Runs will allow age related selection criteria for elder abuse
  - Real time log management vs. report

AuditLink

What's Next



What's Next

- Early December web conference to review:
  - Procedures for account opening and attaching risk ratings to member accounts
  - Analyzing member activity and risk rating members according to due diligence
  - Implementing PIB
  - Opening up the Audit Link site to share policies and procedures
- Mid January web conference for reviewing examination checklist and peer processes and policies (collaborative with CU*Answers clients)

Questions?

LEGAL DISCLAIMER

The information contained in this email does not constitute legal advice. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this email. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.