# Evolving Information Security Challenges

A Cautionary Tale

Plus

Cross-Channel Risk

Dan Tobin

IT Examiner

Supervision, Regulation & Credit

Dan.tobin@bos.frb.org

FEDERAL RESERVE BANK OF BOSTON™

# Agenda

- A Cautionary Tale
  - Shames-Yeakel v. Citizens Financial Bank
- Cross-Channel Risk

# Shames-Yeakel v. Citizens Financial Bank, IL Decision of August 21, 2009

- The plaintiffs obtained a HELOC from bank
- In 2007, online accounts accessed using plaintiffs username and password.
- $26,500 advance on the HELOC, transferred to a bank in Austria.
- Austrian bank refused to return the money.

# Shames-Yeakel v. Citizens Financial Bank Finger-Pointing

- Bank held customers liable for the loss, per the online banking agreement.
- Bank began to bill the customers for the $26,500.
- Bank threatened to foreclose.

# Shames-Yeakel v. Citizens Financial Bank Heads to Court

- The couple sued the bank, claiming violations of the Electronic Funds Transfer Act and the Fair Credit Reporting Act.

- In addition to these claims, the plaintiffs also accused the bank of negligence under IL state law.

# Shames-Yeakel v. Citizens Financial Bank Protection of Customer Information

- Basis for their negligence claim: financial institutions have a duty to protect their customers' confidential information against identity theft.

- "If this duty not to disclose customer information is to have any weight in the age of online banking, then banks must certainly employ sufficient security measures to protect their customers' online accounts."

# Shames-Yeakel v. Citizens Financial Bank Multi-Factor Authentication

- The plaintiffs argument: Citizens' authentication - ID and password - not state of the art at the time of the theft. It could have used "multifactor identification"
- Referenced 2005 FFIEC guidance

# Shames-Yeakel v. Citizens Financial Bank Lesson To Be Learned?

- August 21, 2009, the Illinois District Court concluded: "*In light of Citizens' apparent delay in complying with FFIEC security standards, a reasonable finder of facts could conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access.*

# What's It All Mean???

Dollars and sense

# Agenda

- A Cautionary Tale
  - Shames-Yeakel v. Citizens Financial Bank
- Cross-Channel Risk

# Definition

Cross-Channel Fraud

- Theft from deposit accounts by way of multiple points of access — whether branch, automated teller machine, call center, debit card, online banking, ACH or wire.

# Cross Channel Risk

- Online, ACH, check, debit, wire — more channels mean more opportunities for fraud
- Look for cross-channel exploits to rise

# Cross Channel Fraud Detection

Why so hard to catch?

- Multiple interactions with distinct touch-points
- Forensic focus is usually on the point of the breach, not the interactions leading up to it
- When accessed only for exploration, the online channel typically doesn't record activity

# Why Is The Risk Growing

- Payments products are increasingly using multiple channels
- Emerging payments products are being adopted by financial institutions.
- The increasing role of third-party processors

# Why Is The Risk Growing

- Operational, information security and legal/compliance risks may not be fully understood

- Growing complexity of systems

# Cross Channel Fraud

Business risk factors:

- Operational Risk
- Financial risk
- Compliance risk
- Reputation risk

# Risk Relevance

- Risk is considered high for institutions of all sizes and complexity providing or developing payments products that use cross channel processing.

# For your consideration

- How does your institution review the risk of new products?
- Do risk assessments consider the legal and compliance risks?

# For your consideration

- Do existing risk management programs effectively identify, control, and monitor loss exposure across payment channels?

- Does your institution's vendor management program review the use of service providers as payments processors?

# For your consideration

- How does your institution manage fraud risk in its multiple channel payments processes and products?

- Are cross-channel payment system risks fully managed through monitoring and controls? Can transaction flow control and audit trails be documented?

# For your consideration

- How is the electronic transfer of information being secured?

- What is the due diligence process in place to select qualified customers (KYC)?

# Reference Material Available

- Regulatory compliance reference materials should center on Regulations E and Z, and BSA/AML.
- FFIEC Retail Payment Systems Booklet
- OCC Merchant Processing Handbook, December 2001
- FFIEC Guidance Addressing Risk Management of Remote Deposit Capture (January, 2009)
- FFIEC IT Examination Handbook – Guidance on Information Security
- FFIEC Booklet: Retail Payment Systems
- GLBA Section 501.a and 501.b – Protection of Nonpublic Personal Information
- Regulation CC
- Check Clearing for the 21st Century Act
- FRB SR 00-4 Outsourcing of Information and Transaction Processing (2-29-2000)
- OCC Bulletin 2001-47: Third Party Relationships – Risk Management Principles (11-1-2000)
- OCC Bulletin 2002-16: Third Party Service Providers (5-2002)
- OCC Bulletin 2004-20: Risk Management of New, Expanded, or Modified Bank Products and Services
- FFIEC IT Examination Handbook – Guidance on Information Security
- FFIEC Booklet: E-Banking, Appendix A – Examination Procedures; Appendix E – Wireless Banking
- FFIEC Booklet: Retail Payment Systems (8-2003)
- FFIEC IT Examination Handbook, Retail Payments System Booklet
- GLBA Section 501.a and 501.b – Protection of Nonpublic Personal Information

# Questions?