

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®



MBA's 93rd ANNUAL CONVENTION & EXPO 2006

OCTOBER 22 • 25 HYATT REGENCY • CHICAGO

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

Securing Customer Data and Your Business

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®



Wolters Kluwer
Financial Services

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®

MORTGAGE BANKERS ASSOCIATION®



Panelists

- Anthony Garritano
 - » Technology Reporter, National Mortgage News
 - Art Tyszka, CMT
 - » Sr. Product Manager, Wolters Kluwer Financial Services
 - John Beeskow
 - » First Vice President, Information Security, Flagstar Bank
 - Gareth Evans
 - » Chief Operating Officer, iSentry, Inc.
 - Todd A. Luhtanen, CMT
 - » President, Dynatek, Inc.
 - Robert J. Schlecht
 - » Director, Industry Technology, Mortgage Bankers Association
-



Security breaches quickly become public knowledge through privacy disclosure legislation and the media¹

- *"XXXXX loses customer data"*, March 1, 2005, Associated Press
 - » Lost backup tape
 - » Names, SSN, account information of 1.2 million Federal employees
- *"XXXXX reports data theft"*, August 27, 2006, The Boston Globe
 - » 3 stolen laptops
 - » Names, DoB, SSN of thousands of customers
- *"XXXXX warns of possible data theft"*, May 5, 2006, Reuters
 - » Computer in transit "lost"
 - » Names, SSN, mortgage loan numbers of customers and prospects
- *"Info on 3.9M XXXXX customers lost"*, June 6, 2005, CNN/Money
 - » Lost backup tape
 - » Names, SSN, account history, loan information about retail customers, and former customers
- *"Update: Another VA computer missing"*, August 8, 2006, Computerworld
 - » A second laptop stolen
 - » Names, DoB, SSN of 38,000 veterans



Fines from data and security breaches can be significant

- *"ChoicePoint to pay \$15 million over data breach", Jan 26, 2006, MSNBC*
- *"DSW Inc. Settles FTC Charges", December 1, 2005, Federal Trade Commission*
 - » DSW's settlement includes implementing a security program and undergoing audits for the next 20 years. DSW's exposure for losses related to the breach range from \$6.5 million to \$9.5 million.
- *"Berkeley Cal issues alert about stolen laptop computer. It contains 98,000 Social Security numbers -- notifications to warn of identity-theft risk."*

March 29, 2005, San Francisco Chronicle

 - » Following the theft a single laptop, UC Berkeley was forced to notify over 1 million individuals of the breach. Just the cost of the notification was over \$2.4 million.



The Cost of Fraud Potentially Resulting From Security Breaches

- Financial
 - \$1 Billion in Fiscal Year 2005
 - \$546 Million in Q1 and Q2 2006
 - 21,994 Suspicious Activity Reports filed in fiscal year 2005
 - 17,000 Suspicious Activity Reports filed in Q1 and Q2 2006
- Reputation
- Stock Prices
- Brand Recognition



The financial services industry is a prime target from data thieves and legislators

- Handle all critical data elements
- Face multiple, redundant regulations
- Constantly under siege from external attacks
- Data security at great risk internally
- Protecting customer data is critical

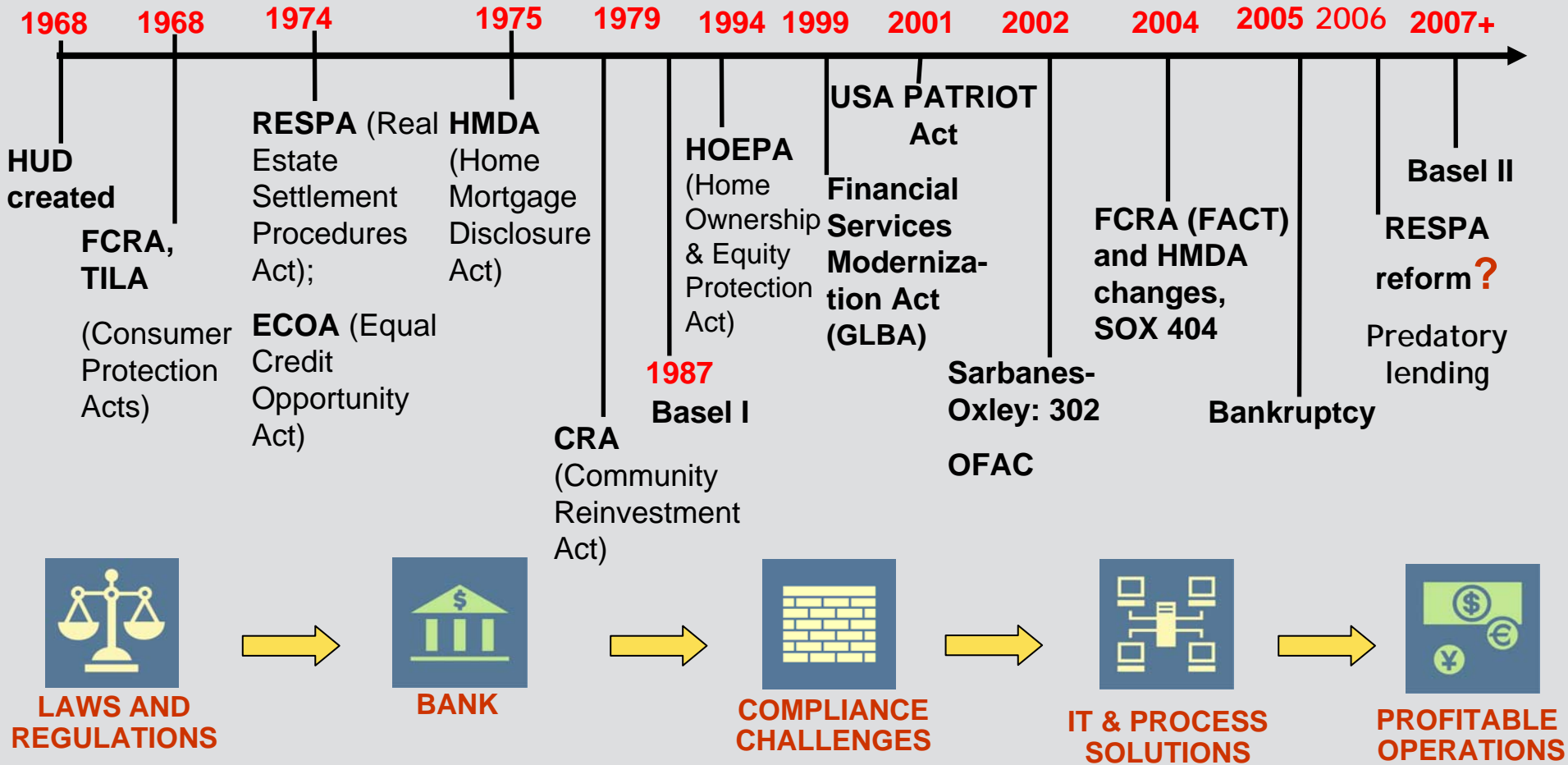


Lenders face the challenge of meeting overlapping legislation

- Legislation
 - » Gramm-Leach-Bliley
 - » Sarbanes-Oxley
 - » Bank Secrecy Act
 - » Federal Financial Institutions Examination Council (FFIEC)
- Careful review of legislation
 - » Meet overlapping requirements with one process



Increasing Regulation : Increasing Complexity





Threats to customer data come from all directions

- External attacks
 - » Direct hacking
 - » Phishing
 - In computing, phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures.²
 - » Pharming
 - Pharming is a hacker's attack aiming to redirect a website's traffic to another (bogus) website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses — they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred as "poisoned". In recent years both pharming and phishing have been used to steal identity information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming. Pharming is becoming the attack du jour of today's hackers.³

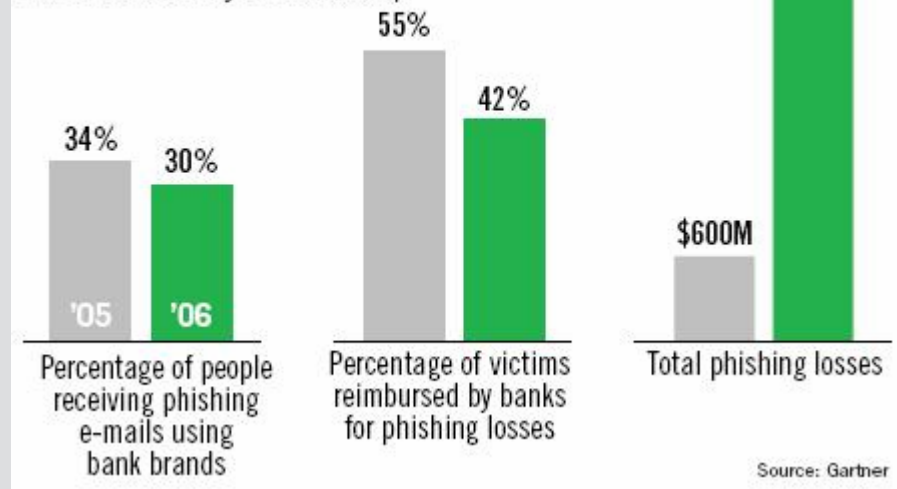


Phishing continues to cost banks and lenders

- Phishing has nearly doubled since 2006⁴
- Consumers who manage to recover some of their losses to phishers are reimbursed by banks 42% of the time⁵
- New FFIEC guidelines call for multi-factor authentication to be in place by Dec. 31, 2006
- Phishing losses are up⁵
 - » \$600 million in 2006
 - » Estimated \$2.8 billion in 2007

Phish Bait

Banks are targeted, and are paying, less often but total industry losses are up





An example of phishing

Online Confirmation Procedure

Dear **Wells Fargo client,**

The Wells Fargo bank Technical Department is performing a scheduled software upgrade to improve the quality of the banking services.
By clicking on the link below you will begin the procedure of the user details confirmation.

<http://www.wellsfargo.com/customerservice/startprocedure/>

These instructions are to be sent to and followed by all Wells Fargo clients.
We apologize for any inconvenience and thank you for cooperation.

Wells Fargo bank Technical Service

© 1999 - 2006 Wells Fargo. All rights reserved. Member FDIC.



Threats to customer data come from all directions

- Internal theft
 - » 70% of all identity theft starts with an employee who has access to customer data
 - Study: ID theft usually an inside job, May 21, 2005, MSNBC
 - Michigan State University study
 - <http://msnbc.msn.com/id/5015565>
 - » Importance of Role-based access



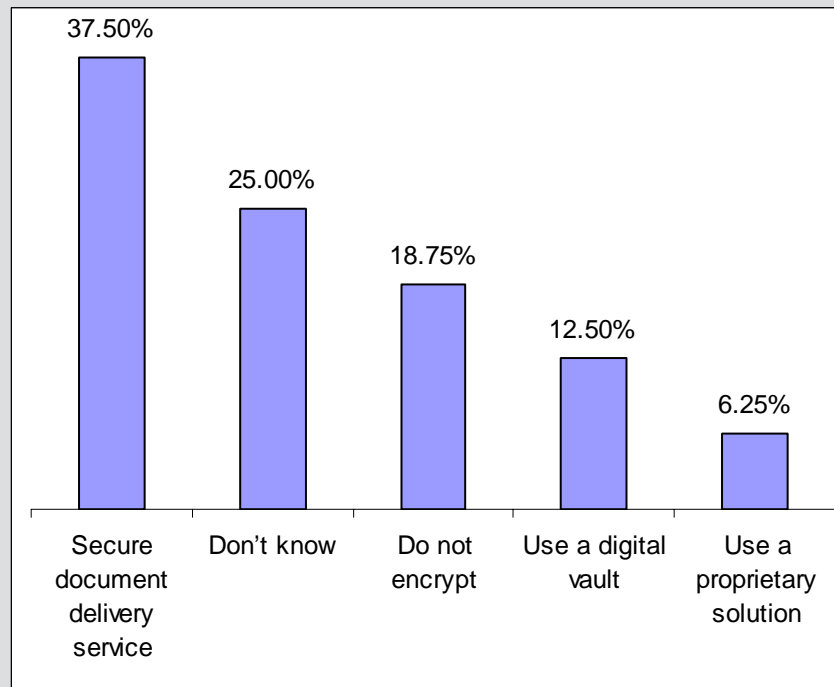
Critical to secure sensitive customer data

- Fines are a reality
 - » ChoicePoint \$15 Million fine⁶
- Reputational risk
 - » Customer trust
- Increased regulation and legislation



Recent Wolters Kluwer Financial Services online poll reveals that many institutions still do not properly secure sensitive data.⁷

- How do you encrypt documents with sensitive data when in storage or transit?





Risk must be minimized and managed to secure data

- Securing data at collection
- Securing data in transit
- Securing data at rest
- Examining current practices
- Striving for best-practices



Create and implement effective security policies

- Manage risk, not eliminate it
 - » Security vs. usability
- Implement
- Audit and test
- Security is an extension of compliance and IT
 - » Not just the responsibility of IT
 - » Compliance and IT need to work collaboratively



Using role-based access further secures data from internal breaches

- Restricting organizational roles
 - » Access only the essential data to perform their job
- Authenticating user identity
 - » Something the user knows (e.g. password, PIN)
 - » Something the user possesses (e.g. ATM card)
 - » Something the user is (e.g. biometric characteristic, such as fingerprint)



Securing data while in transit and at rest

- Encrypting content
 - » PKI
 - » SSL
 - » VPN
 - » Tamper sealing
- Digital Rights Management (DRM)
 - » Flexibility and enforceability



Institute procedural security within the organization

- Require clean desk policies
- Register visitors and use timed passes
- Encourage an atmosphere of awareness
 - » Training
 - » Whistle blowing



Test applications and processes regularly

- Look for weaknesses
 - » Best-in-class security in 2000 may be inadequate in 2006
- Be aware of your vendor's policies
- Outsource penetration testing
 - » Hire "Ethical Hackers"
 - » Vendors like Symantec
- Put your employees to the test



Protecting customer data is protecting your business

- Secure sensitive data
 - » From the outside and inside
- Define and implement security policy
 - » Examine all regulations
- Test and evaluate security policy
- On-going sharing of best-practices
 - » Participation in industry groups
 - » Communication with peers



Panelists

- Anthony Garritano
 - » Technology Reporter, National Mortgage News
 - Art Tyszka, CMT
 - » Sr. Product Manager, Wolters Kluwer Financial Services
 - John Beeskow
 - » First Vice President, Information Security, Flagstar Bank
 - Gareth Evans
 - » Chief Operating Officer, iSentry, Inc.
 - Todd A. Luhtanen, CMT
 - » President, Dynatek, Inc.
 - Robert J. Schlecht
 - » Director, Industry Technology, Mortgage Bankers Association
-