

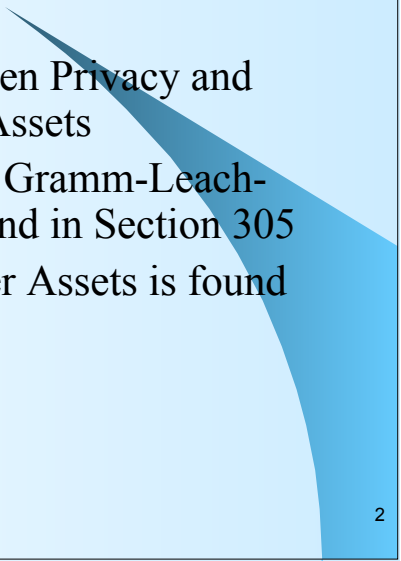
Safeguarding Customer Assets

OTS

A decorative blue gradient shape that starts as a thin point on the left and expands into a wider, curved shape towards the right, located in the bottom right corner of the slide.

1

Introduction

- Industry confusion between Privacy and Safeguarding Customer Assets
 - Privacy provisions of the Gramm-Leach-Bliley (GLB) Act are found in Section 305
 - Safeguarding of Customer Assets is found in GLB Section 501(b)
- 
- A decorative blue gradient shape that starts as a thin point on the left and expands into a wider, curved shape towards the right, located in the bottom right corner of the slide.

2

Why are technology security risks increasing

- Access to information is demanded by customers and visible to customers
- Reputation risk can spread panic
- Service Providers security systems can be immature
- Underlying technology is built on openness
- Changing privacy culture and regulations
- Economics of implementing security framework
- A lack of security requirements definition
- Resource Constraints

3

Panelists:

- Privacy and Data Security
 - Jane Anne Schmoker – FRB Dallas
 - Jane.A.Schmoker@dal.frb.org
- Safeguarding Customer Information Provisions
 - Steven L. Martin – Texas Department of Banking
 - Smartin@banking.state.tx.us
- One Year Later – A Regulator’s Perspective
 - James O. Brignac – FDIC
 - Jbrignac@fdic.gov
- FFIEC Information Security Booklet
 - W. Carter Messick – OCC
 - Carter.messick@occ.treas.gov

4

Privacy & Data Security

Interagency IT Security Conference
October 15-17, 2002

Jane Anne Schmoker
Senior Counsel
Federal Reserve Bank of Dallas

5

Lexis-Nexis P-TRAK Database

- On June 1, 1996, Lexis-Nexis introduced P-TRAK.
- On June 11, removed the social security numbers.
- September, receiving thousands of telephone calls about P-TRAK.
- Congress asks FTC to investigate information-containing computerized databases.

6

US Bancorp Case

- The Minnesota Attorney General sued U.S. Bancorp alleging that the bank sold customer information to a 3d party telemarketing firm in violation of the FCRA.
- US Bancorp agreed not to transmit customer information to non-affiliates for non-financial services and to disclose privacy policies and allow “opt out” on information sharing for all financial services.

7

EU Privacy Provisions

- Adopted a Directive on Data Protection, October 24, 1995, effective 1998.
- Prevents transfer of personal data outside the EU to countries lacking adequate levels of data protection.
- Applies to all data processing and all organizations holding personal data.

8

Safe Harbor

- Companies must notify consumers of purpose of data collection.
- Must also allow consumers opportunity to opt out of data sharing.
- Must provide access to their personal information.

9

Privacy Regulations

- OCC - 12 CFR §40
- Federal Reserve - 12 CFR §216
- FDIC - 12 CFR §332
- OTS - 12 CFR §573
- NCUA - 12 CFR §716
- SEC - 17 CFR §248
- CFTC - 17 CFR §160
- FTC - 16 CFR §313

10

Privacy Regulations

- Financial institutions would have to disclose privacy policies to customers -
- Before the relationship is established and at least annually thereafter.
- Financial institutions may not directly or through an affiliate disclose to nonaffiliates any nonpublic personal information without prior notice to a consumer.

11

Protected Information

- Nonpublic Personal Information - personally identifiable information.
- Does not include publicly available information.

12

Personally Identifiable Information

Financial information that

- is provided by a consumer to a bank
- results from any transaction with the consumer
- is obtained in performing a service for the consumer or otherwise obtained by the bank.

13

Financial Information

- Any information requested by a bank for the purpose of providing a financial product or service.
- Includes the fact that a particular person has a customer relationship with an institution.

14

Publicly Available Information

Information the bank has a reasonable basis to believe is lawfully made available to public

- From official public records
- Information widely distributed by media - OR
- Disclosures to general public required by law.

15

Notice of Privacy Policies

- Categories of information that may be **collected**.
- Categories of information that may be disclosed.
- Categories of affiliates and nonaffiliates to whom the institution discloses information

16

Notice of Privacy Policies

- Policies and practices regarding disclosure of information on former customers.
- Explanation of right to opt out and instructions to exercise the right.
- Information about how institution protects information.

17

Safeguarding Customer Information

Interagency IT Security Conference
October 15-17, 2002

Steven L. Martin

Senior Assistant General Counsel
Texas Department of Banking

18

SAFEGUARDING CUSTOMER INFORMATION

- GLB requires Federal regulatory agencies to establish standards related to administrative, technical, and physical safeguards of customer information.

19

SAFEGUARDING CUSTOMER INFORMATION

- Standards should:
 - Ensure security/confidentiality of customer records;
 - Protect against threats/hazards to security and integrity of records; and,
 - Protect against unauthorized access to or use of records.

20

SAFEGUARDING CUSTOMER INFORMATION

- OCC - 12 CFR Part 30, Appendix B
- Federal Reserve -
 - 12 CFR Part 208, Appendix D-2
 - 12 CFR Part 225, Appendix F
- FDIC - 12 CFR Part 364, Appendix B
- OTS - 12 CFR Part 570, Appendix B
- NCUA - 12 CFR Part 748, Appendix A
- FTC - 16 CFR Part 314

21

DEFINITIONS

- “**Board of Directors**” – in the case of a foreign bank branch or agency means the managing official.
- “**Customer**” defined as in privacy regulations.
- “**Service provider**” – person or entity that is permitted access to customer information through its provisions of services directly to financial institution.

22

INVOLVE THE BOARD OF DIRECTORS

The Board shall:

- Approve the written information security program.
- Oversee the development, implementation, and maintenance of the financial institution's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

23

ASSESS RISK

Each financial institution shall:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
- Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

24

MANAGE AND CONTROL RISK

- Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the financial institution's activities.
- Train staff to implement the information security program.
- Regularly test the key controls, systems, and procedures.

25

OVERSEE SERVICE PROVIDERS

- Due diligence
- Require by contract to implement measures designed to meet the objectives of the Guidelines.
- Monitor – review audits, test result summaries, etc.

26

MONITOR, EVALUATE, AND ADJUST THE PROGRAM

- Changes in technology
- Sensitivity of customer information
- Internal or external threats
- Changing business arrangements

27

501(b) - One year later (A regulators perspective)

**James O. Brignac, FDIC
Information Systems Exam Specialist
2002 Inter-Agency
IT Security Conference
October 17, 2002**

28

FDIC Examiner Survey

- DOS follow-up usually done within 1 year of new requirement
- Survey sent to every field office in all 8 regional offices
- 5 questions
- Informal survey, not intended to be “scientific”

29

FDIC Examiner Survey

- Survey Questions:
 - 3 most common deficiencies
 - Most common question asked by bankers
 - Is there confusion between privacy regulation and security guidelines?
 - How much time have banks spent complying?
 - How long for examiners to complete this part of exam?

30

Three Most Common Deficiencies

1. Inadequate risk assessment
 - Slightly more than half of responses noted banks with no assessment
2. Inadequate security policy/program
 - About one-third of responses noted banks with no written security policy
3. Inadequate: Board involvement, testing, training

31

Most Common Banker Questions

1. How should a bank perform & document a risk assessment?
2. Does FDIC have any further guidance on what an acceptable risk assessment & security policy should look like?
 - What guidelines?
 - Am I in compliance?
 - What are other banks doing?

32

Confusion With Privacy Regulation

- **YES**
- Overall, very large percentage of survey forms said that bankers confuse privacy regulation & security guidelines
- Some bankers think they are same thing
- Some bankers think compliance with privacy regulation means compliance with security guidelines

33

Time Spent Complying

- No significant expenditure of time so far (see previous slides)
- Banks anticipate significant time going forward
- Large v. small banks
- Some \$ spent, mostly time
- Some are comparing burden to Y2K

34

Time Spent by Examiners

- Nationwide overall average: about 1-1/2 days
- Significantly less for banks with no security program and very small banks
- More time for banks with a security program and large banks

35

Recommendations

- Become familiar with what the guidelines require
- Conduct & document a formal, comprehensive risk assessment
- Develop a written security policy/program
- Brief the Board of Directors and get their approval

36

James O. Brignac
IS Examination Specialist
Dallas Regional Office

jbrignac@fdic.gov

37

FFIEC Information Security
Booklet

W. Carter Messick, OCC
Interagency IT Security Conference
October 15-17, 2002



38

Agenda

- Background
- Goals
- Preview of Content
- Status

39

Background

- Part of 1996 IS Handbook updating
- Environmental Changes Since 1996
 - Growth in networks and distributed systems
 - Explosion in external access (e.g. Internet)
 - Extensive usage of COTS products rather than custom SDLC designs.
 - Extensive reliance on unreliable protocols and software
 - GLBA and increased privacy concerns

Result: Potential for increased risk!

40

Background

- Aimed at the mid-level IT examiner
 - Assumes knowledge of basic concepts and technologies.
 - Assumes ability to tailor exam procedures for a specific examination.

41

Goals

- Focus on risk and risk management
 - Consistent with other examination approaches
 - Focuses on PROCESS, not state or condition of controls

Examination is NOT

- Penetration assessment,
- Penetration test, or
- Audit

42

Goals

- *Mirror and expand* on the GLBA 501(b) approach.
 - Leverage the GLBA security process
 - Provide additional and more complete explanations of the process elements

43

Goals

- Create consistent information security expectations for financial institutions and service providers.



44

Booklet Preview

- Narrative
 - Introduction
 - Security Process (including roles and responsibilities)
 - Information Security Risk Assessment
 - Information Security Strategy
 - Security Controls Implementation
 - Security Testing
 - Monitoring and Updating
- Exam Procedures

45

Risk Assessment

- Functional requirements
 - Information gathering
 - Analysis
 - Inventory system assets and components
 - Identification and measurement of threats
 - Threat scenarios
 - Likelihood of occurrence and damage
 - Prioritize controls, monitoring, and testing to prevent, detect, or correct events.
- Key administrative practices
 - Multi-disciplinary
 - Systematic and centrally controlled
 - Integrated
 - Accountable
 - Documented
 - Knowledge-enhancing
 - Flexible and Updated

46

Security Testing

- Many possible tests
- Types of independent tests
 - Audit
 - Vulnerability assessment
 - Penetration test
- Function
 - Testing plan based on risk
 - Controls to mitigate testing risks
 - Use test results to re-assess whether objectives are met.

47

Examination Procedures

- Procedures are objective based, in 2 tiers
 - Tier 1 is meant for a quick overview of the risk and risk management process
 - Tier 2 is detailed verification procedures
- Procedures take a tool-kit approach, examiners should tailor procedures to individual institution.

48

Status

- Field Testing Complete
- Edits Underway
- Still need senior interagency review
- Issuance planned for November or December 2002



49

Q&A Panel

James Brignac - FDIC

jbrignac@fdic.gov

Mary Carole Ducharme - OTS

mary.ducharme@ots.treas.gov

Carter Messick - OCC

carter.messick@occ.treas.gov

Jane Anne Schmoker - FRB Dallas

jane.a.schmoker@dal.frb.org

Steven L. Martin - Texas Department of Banking

smartin@banking.state.tx.us



50