48,412

TIGER TESTING
The Independent Computer Security Testing Specialists

6

Tiger Testing's Comments on the Proposed Guidelines Establishing Standards for Safeguarding Customer Information Published to Implement Section 501 and 505(b) of the Gramm-Leach-Bliley Act.

Comments submitted August 24, 2000 by

Ken Brandt, Managing Director, Tiger Testing
30 Wall Street, New York, NY 10005, www.TigerTesting.com, (212) 898-9322

For the
Department of the Treasury
Office of he Comptroller of the Currency
12 CFR Part 30
(Docket No. 00-13)
RIN 1557-AB84
and
Federal Reserve System
12 CFR Parts 208, 211, 225, 263
(Docket No. R-1073)
and
Federal Deposit Insurance Corporation
12 CFR Parts 308 and 364
RIN 3064-AC39
and
Department of the Treasury
Office of Thrift Supervision
12 CFR Parts 568 and 570
(Docket No. 2000-51)
RIN 1550-AB36

This following is Tiger Testing's response to the June 26, 2000 joint agency request for comments on the proposed Guidelines establishing standards for safeguarding customer information published to implement section 501 and 505(b) of the Gramm-Leach-Bliley Act. Tiger Testing has extensive expertise and a unique perspective on this issue because our firm's sole business is to test the security of web sites and their underlying systems.

The agencies request for comments is indicated below by a Q, and Tiger Testing comments are indicated below by an A.

30 Wall Street, New York, New York 10005
www.TigerTesting.com
Phone (212) 898-9322 Fax (212) 361-2209 E-Mail kbrandt@tigertesting.com

Overall

Q: General view of the proposed regulations & guidelines?

A: Tiger Testing favors the proposed regulations because they require regular external web site security testing, which is a critical component of safeguarding customer records and information.

Section II – Standards For Safeguarding Customer Information
Section IIA – Involve the Board of Directors and Management

Q: How frequently should management report security issues to the board of directors?

A: Tiger Testing believes that security testing should be continuous and on-going, and that the results should be reported monthly. Continuous and on-going testing of security is required because safeguards to customer records and information could fail at any time. This can happen as a result of: either simple changes to a financial institution's systems, or (unfortunately) continuous advances in computer hacker technology. Monthly reporting of security issues would give management enough time to react to new security gaps by bolstering safeguards to customer records. In this way management's reports to the board could include the system security and privacy issues uncovered, as well as the steps being taken to safeguard customer information. Addressing open system security issues on a timely basis is critical to safeguarding privacy. Less frequent reporting would potentially slow management's response.

Q: Should the position of Corporate Information Security Officer (with appropriate authority) be mandated?

A: For the same reasons that individual investors are protected by internal financial auditors and outside financial auditors, individual customers should be protected by an internal corporate information security specialists and external security firms. Independent internal and external checks on security would significantly increase the likelihood that system security and the associated customer privacy vulnerabilities are identified and addressed.

30 Wall Street, New York, New York 10005
www.TigerTesting.com
Phone (212) 898-9322 Fax (212) 361-2209 E-Mail kbrandt@tigertesting.com

Section III – Develop and Implement Information Security Program
Section IIIC – Manage and Control Risk

Q: Should specific types of security tests (i.e. penetration testing) be specified?

A: Yes – penetration testing should be specified. Systems designed to protect the security of customer information are similar to all other systems: when they are changed or when they are expected to handle external changes (i.e. continuous advances in computer hacker technology), they should be tested. Continuous penetration testing is the only way to know if the financial institution's comprehensive risk management plan is being updated, implemented and protecting customer information.

Q: Should the tests be performed by persons who are not employees of the financial institution?

A: Yes - customer information is better protected by external testing than internal testing because:

- Greater Expertise - External testing firms fund on-going R&D, systems development, and operations to maintain and run state-of-the-art proprietary security testing tools and techniques. It would not be cost effective to fund such an effort for internal testing alone.
- Cost Effective - Internal system security staffs have a limited amount of time and a limited budget. Financial firms that use external system security tester can devote a greater amount of their internal system security team's time to closing and preventing security gaps to safeguard customer privacy.
- Lack of Corporate Bias – External testers would be more effective than internal testers because external testers would not be biased by a financial firm's: previous system security decisions, current system environment, or future system security plans.
- Full Reporting – Employees of financial firms may be reluctant to report security gaps because they believe that: presenting any bad news would be bad for their career, the gaps might have been caused by them, and/or the gaps might have been caused by their friends. Conversely, career advancement and professional recognition at external testing firms is dependent upon identifying security gaps.

30 Wall Street, New York, New York 10005
www.TigerTesting.com
Phone (212) 898-9322 Fax (212) 361-2209 E-Mail kbrandt@tigertesting.com

Q: What is the appropriate degree of independence?

A: Customer information is better protected by independent testers that do not have any conflicts of interest:

- Independence assures unbiased and complete test results.
- Firms that sell: auditing, consulting, software, hardware, firewalls, hosting, or networking services or products have conflicts of interest.
- In order to best safeguard consumer privacy, system security should be tested by independent security testers with no conflicts of interest.

IIID – Oversee Outsourcing Arrangements

Q: What is the appropriate treatment of outsourcing arrangements?

A: Outsourced systems designed to protect the security of customer information are similar to all other systems: when they are changed or when they are expected to handle external changes (i.e. continuous advances in computer hacker technology), they should be tested. Continuous penetration testing is the only way to know if customer information is being safeguarded.

30 Wall Street, New York, New York 10005
www.TigerTesting.com
Phone (212) 898-9322 Fax (212) 361-2209 E-Mail kbrandt@tigertesting.com