

# **TIGER TESTING**

The Independent Computer Security Testing Specialists

October 3, 2000

Secretary  
Federal Trade Commission  
Room H-150  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

*sent via e-mail only to: GLB501Rule@ftc.gov*

Re

**Tiger Testing's comments on the Privacy Safeguards Rule  
Gramm-Leach-Bliley Act, Privacy Safeguards, Rule 16-CFR Part 313-Comments**

Dear Federal Trade Commission:

Introduction

The Internet has increased the risk of lost customer and consumer privacy. Tiger Testing has extensive expertise and a unique perspective on this issue because privacy is dependent upon security, and our firm's sole business is to test the security of web sites and their underlying systems.

In order to meet the Act's and the FTC's requirements of addressing:

- a) Anticipation of Threats or Hazards to Security or Integrity,
- b) Preventing Unwarranted Access and Use, and
- c) Insuring Security and Confidentiality,

the FTC rule should require ongoing security testing (including web site penetration testing) by an independent outside testing firm.

On-Going Security Testing (including Penetration Testing) To Insure Privacy

Tiger Testing's clients believe 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 and consumer 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

- Page 1 of 3 -

# TIGER TESTING

The Independent Computer Security Testing Specialists

technology. Monthly reporting of security issues would give management enough time to react to new security gaps by bolstering safeguards to customer and consumer records. Addressing open system security issues on a timely basis is critical to safeguarding privacy. Less frequent reporting would potentially slow management's response.

## External Security Testing (including Penetration Testing) To Insure Privacy

Many financial institutions do an excellent job of testing the security, and insuring the integrity of their customer and consumer privacy. Nevertheless, customer and consumer privacy is better protected by external testing than internal testing because:

- Greater Expertise - External testing firms, such as Tiger Testing, fund on-going R&D, systems development, and operations to maintain and run state-of-the-art security testing tools and techniques. A financial firm could not justify the effort to develop and maintain such expertise for internal testing.
- Cost Effective – Financial firm's security staffs have a limited amount of time and a limited budget to devote to testing. Financial firms that use an 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. It would not be cost effective for financial firms to fund such an effort for internal testing alone.
- Lack of Corporate Bias – External testers would be more objective 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 disclose security gaps because they may believe that: presenting any bad news may 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 such as Tiger Testing are dependent upon identifying security gaps.

## Independent Security Testing (including Penetration Testing) To Insure Privacy

Customer and consumer privacy is best 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.

# **TIGER TESTING**

**The Independent Computer Security Testing Specialists**

## Summary

The most effective way for the FTC to safeguard customer and consumer privacy is to require ongoing security testing (including web site penetration testing) by an independent outside testing firm.

Ken Brandt  
Managing Director

- Page 3 of 3 -

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