



Gramm-Leach-Bliley Security Requirements: Keeping Robbers and Regulators from the Door

```
RP C Wnc  
THER Typ  
RP C Wnc  
468x60;s
```

```
s=<nop,nop,ts  
pe=0806 (ARP),  
o is 10.0.0.42  
pe=0806 (ARP),  
o is 10.0.0.42
```

```
{3249>
```



By Daniel J. Langin

Introduction

Many years ago, a famous bank robber, when asked why he robbed banks, said “that’s where the money is.” That answer may have betrayed more about the robber’s sense of humor than the desirability of bank robbing, given that he made this statement during the greatest wave of bank failures in U.S. history. Bank regulation and reform since then have created a strong and vibrant financial services industry, but unfortunately, hackers and information thieves have continued to follow the bank robber’s advice.

Faced with a continuing increase in breach of security incidents affecting financial institutions, the government ultimately passed the Gramm-Leach-Bliley Act (“GLB”), which regulates the privacy and protection of customer records maintained by financial institutions. Although a great deal of attention has been focused on the privacy requirements of GLB, a lesser known (but perhaps more important) set of requirements exists under GLB. These are the *information security* requirements known as the “financial institution safeguards.”

Information Security Requirements Under GLB: Overview and Board Responsibility

Essentially, GLB authorizes the agencies that regulate financial institutions (FTC, SEC, etc.) to create information security standards for the institutions. Section 501(b) of GLB states:

(b) Financial institution safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical and physical safeguards—

- (1) to insure the security and confidentiality of customer records and information;
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer¹.

As required by this section of GLB, the agencies have now issued the “Interagency Guidelines Establishing Standards for Safeguarding Customer Information” (the Guidelines), which create common standards for financial institution security. According to a May 31, 2001 letter from the Federal Reserve System, financial institution examiners are to “assess compliance with the Guidelines during *each safety and soundness examination or examination cycle* (which may include *targeted reviews of information technology*) . . . and *monitor ongoing compliance* as needed . . .” (Emphasis added). In other words, whether as part of regular institution examinations or “targeted reviews,” federal examiners must now review the information security status of the institution.

The Guidelines specifically name the financial institution’s board of directors as the primary body responsible for information security. Section III.A. states that the board or a committee of board members is required to approve the bank’s security policy, and to “oversee the development, implementation, and maintenance of the bank’s information security program, including assigning specific responsibility for its

² 15 U.S. Code Section 6801(b).

³ Published at [Federal Register](#) Vol. 66, No. 22, February 1, 2001, pp. 8616-8641.

implementation and reviewing reports from management³.” Although a number of institutions apparently asked the agencies to tone down this portion of the Guidelines and to substitute management instead of the board as the primary entity responsible for information security, the agencies refused, and reinforced the board’s duties in the following commentary to the Guidelines:

Some commentators stated that each financial institution should be allowed to decide for itself whether to obtain board approval of its program [for information security]. . . . Still others suggested modifying the Guidelines to require only that the board approve the initial information security program and *delegate subsequent review and approval of the program to either a committee or an individual*. The Agencies believe that a financial institution’s overall information security program is critical to the safety and soundness of the institution. Therefore, *the final Guidelines continue to place responsibility on an institution’s board to approve and exercise general oversight over the program*⁴. (Emphasis added).

Section III.F. of the Guidelines requires the board to review its information security measures annually. The commentary to the Guidelines clarifies that day to day handling of information security matters can be delegated to management, but the core message is clear: The financial institution’s board of directors has the primary, non-delegable duty for meeting the information security requirements under the Guidelines.

What Information Security Measures Do the Guidelines Require?

Section III.C.1. of the Guidelines requires financial institutions to adopt the following measures to the extent that they are likely to protect customer information:

- a. Access controls on customer information systems;
- b. Access restrictions at physical locations containing customer information;
- c. Encryption of electronic customer information;
- d. Procedures to ensure that system modifications do not affect security;
- e. Dual control procedures, segregation of duties, and employee background checks;
- f. Monitoring systems to detect actual attacks on or intrusions into customer information systems;
- g. Response programs that specify actions to be taken when unauthorized access has occurred; and
- h. Protection from physical destruction or damage to customer information.

Although the Guidelines by and large do not require institutions to use specific products, the agency Examination Procedures specifically advise examiners to look for IDS in connection with item f above:

Review monitoring systems and procedures, *including network and host intrusion detection systems*, network traffic monitoring, manual reviews of logs and other information available to assess management’s monitoring process. (Emphasis added)

These Examination Procedures were created by the agencies as a checklist for examiners to use when determining whether institutions meet GLB requirements under the Guidelines. Although the Guidelines have been in effect since July 1, 2001, many institutions may only now be preparing for their regular agency examinations. Given that IDS is one of only two specific technologies that the Examination Procedures identify (the other is encryption), the relative weight that examiners assign to an IDS may become very important during a review of the institution’s GLB compliance.

³ See, e.g., The Guidelines as adopted by the Office of Comptroller of the Currency, at 12 CFR I, Appendix B to Part 30.

⁴ See “Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness,” Part III, published at Federal Register Vol. 66, No. 22, February 1, 2001, at 8620.

Damages, Fines and Penalties Under GLB

Under GLB Section 505, the agencies may enforce GLB with the same sanctions that they currently use to regulate financial institutions. For example, the FDIC may enforce violations under Section 8 of the Federal Deposit Insurance Act, which gives the FDIC the authority to impose penalties ranging from \$5,000 per day up to \$1,000,000⁵. GLB Sections 521 and 523 also provide enhanced criminal penalties for persons who gain fraudulent access to protected financial information.

Conclusion

Unlike the bank robber mentioned in the Introduction to this article, today's criminals do not always need to burst in the front door toting a machine gun. Protections such as an IDS and the other measures required by GLB can keep both robbers and regulators from causing losses to financial institutions.

Dan Langin (dlangin@msn.com) is a lawyer with 8 years of experience providing legal advice and consulting to information technology, information security and insurance companies on Internet and technology law. He provides counsel in his private practice, in affiliation with TechRiskLaw.com, and as corporate counsel to several technology companies. Dan has actively spoken and participated in business roundtables on technology legal issues in the U.S., Canada, Ireland, the European continent and Israel. He has been quoted in [USA Today](#) and numerous insurance and technology industry publications. This article is not intended as legal, risk management, consulting or other advice, whether with respect to the use of any Recourse Technologies, Inc. products or otherwise. It contains the author's personal observations concerning general factual circumstances and broad legal issues rather than specific factual or legal situations, and does not reflect the views of Recourse Technologies, Inc. or any current or past employers or clients. Persons wishing to obtain legal, risk management, consulting or other advice on these or other topics, or on specific factual circumstances involving the issues discussed in this paper, should contact a subject matter professional of their choice.

⁵ 12 U.S. Code Section 1818.



WE GIVE YOU RECOURSE AGAINST HACKING

1.877.786.9633

info@recourse.com

www.recourse.com

Copyright © 2002 Recourse Technologies, Inc. All rights reserved. Recourse, ManTrap and ManHunt are trademarks of Recourse Technologies, Inc. All other registered or unregistered trademarks are the sole property of their respective owners.