Message from the Chair

This is the inaugural edition of the eNewsletter for the Banking Law Committee, and warmest thanks need to be extended to Chris Bellini, Editor, and to Peter Heyward, Tom Vartanian, Charlotte Bahin, and Ray Natter, his intrepid columnists, for pulling together the handsome and entertaining inaugural edition. So far, they are all protecting their sources and none has been threatened with serious time in jail — a little “inside the Beltway” humor during the Dog Days of August.

There are many ways to be involved in the Banking Law Committee’s activities. Many members of the Committee chose to attend the Fall, Spring, and/or Annual Meetings and appreciate the quality and depth of the information that is shared at our Programs, Committee Forum, and Subcommittee meetings. We are justifiably proud of the high level of programming that the Committee regularly sponsors, especially our “crown jewel” Fall Meeting usually located near the Washington, D.C. metropolitan area to permit the participation of many senior members of the Federal banking agencies.

The purpose of the eNewsletter is to communicate with the members of the Committee about reasonably current events between those meetings, and to communicate with those members of the Committee who, for whatever reason, are not able to participate in the meetings as often as they would like to.

The current plans envision publication of the eNewsletter on a quarterly basis while the Editor and his columnists get used to their new responsibilities. It may be possible to entertain “guest” columns from members of the Banking Law Committee after the Editor and his columnists get all of the “bugs” out of the production system. Please contact Chris Bellini, cbellini@gibsondunn.com, with any comments or suggestions that you may have about the eNewsletter.

---

Featured Articles

Citigroup to Congress: Never Mind! (Some reflections on the Gramm-Leach-Bliley Act prompted by Citigroup’s exit from insurance underwriting)

Peter E. Heyward

There is an obvious irony in Citigroup’s decision, announced in February, to sell most of its life insurance business, thus largely completing an exit from the insurance underwriting business that began with the spin-off to shareholders of its property and casualty operations in 2002. Citigroup, as a financial conglomerate combining banking, securities and insurance in a single holding company, had been both the midwife and the most obvious beneficiary of the Gramm-Leach-Bliley Act (“GLBA”), whose enactment in 1999 (as opposed to, say, 2019) was undoubtedly hastened by The Travelers Group’s bold acquisition of Citicorp the year before. Pared down essentially to banking, securities and insurance agency activities, Citigroup could have

---

Martin E. Lybecker

Wilmer Cutler Pickering Hale and Dorr LLP
2445 M Street, N.W.
Washington, D.C. 20037
(202) 663-6240
martin.lybecker@wilmerhale.com

---

Citigroup to Congress: Never Mind! (Some reflections on the Gramm-Leach-Bliley Act prompted by Citigroup’s exit from insurance underwriting)

Peter E. Heyward

There is an obvious irony in Citigroup’s decision, announced in February, to sell most of its life insurance business, thus largely completing an exit from the insurance underwriting business that began with the spin-off to shareholders of its property and casualty operations in 2002. Citigroup, as a financial conglomerate combining banking, securities and insurance in a single holding company, had been both the midwife and the most obvious beneficiary of the Gramm-Leach-Bliley Act (“GLBA”), whose enactment in 1999 (as opposed to, say, 2019) was undoubtedly hastened by The Travelers Group’s bold acquisition of Citicorp the year before. Pared down essentially to banking, securities and insurance agency activities, Citigroup could have
operated under the pre-GLBA bank regulatory structure, albeit with some inconvenience.

More...

**The Industrial Loan Company Controversy**
*Raymond Natter*

For the past several years, legislation to reduce regulatory burden in the financial services industry has been repeatedly bogged down by a controversy involving a little known type of financial intermediary — the "Industrial Loan Company" or "ILC." These institutions represent one of the few remaining methods by which a commercial company may own an insured depository institution, and efforts to exclude these companies from more general regulatory relief legislation has rekindled the debate over mixing banking and commerce. In part this arose from a proposal made by Wal-Mart in 2002 to charter a new ILC in California, and use this institution to provide financial services in its stores. This article will review the history and current legal status of industrial loan companies.

More...

**Information Security: Principles and Best Practices**
*Thomas P. Vartanian, Mark Fajfar, Robert H. Ledig*

Ever easier access to electronic information systems has fueled an explosion of new products and services available at remote locations via the Internet. Sophisticated transactions are no longer confined to the back office. This dependence on remote access to electronic information systems requires a compromise between accessibility and security, since the very process of making a system widely accessible will lessen its security. From a legal perspective, information security principles and best practices are discerned from regulatory guidance and legal precedents as to the proper course to follow in counteracting information security threats.

What Are the Threats to Information Security?

More...

**Banking Agencies Issue Guidance on Response Programs for Unauthorized Access to Customer Information**
*Charlotte M. Bahin*

**Introduction**

With increased frequency, the confidential personal information of customers of various entities has been compromised. Generally, the breaches to date have not involved an insured institution directly, but have resulted from an action or inaction of a third party. Nonetheless, in several well-publicized situations, it is the financial institution with which many customers have contact and to whom they look to for recourse.

In 2003, the federal banking agencies issued a proposal that would interpret Section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act") and supplement the Interagency Guidelines Establishing Information Security Standards (Security Guidelines). This interpretation and supplement is the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (final guidance). The final
guidance establishes a risk-based framework for financial institutions to develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider.

More...

House Bill Provides For A More Bank-Like Regulator For Fannie and Freddie
Raymond Natter

On May 25, 2005, the Financial Services Committee of the U.S. House of Representatives overwhelmingly approved a bill, H.R. 1461, to strengthen the supervision and regulation of Fannie Mae and Freddie Mac (the “GSEs” or the “Enterprises”). The bill has engendered some controversy based, in part, on provisions that could be used to enhance the GSE’s competitive position, such as increases in the size of loans that Fannie Mae and Freddie Mac can purchase. Arguments have also been made that the regulatory and safety and soundness provisions in the bill are too weak, and that these areas of the bill are “worse than current law.” This article will address this second point only, and will compare the regulatory and safety and soundness authority of the GSE’s current regulator, the Office of Federal Housing Enterprise Oversight (OFHEO) with the authority that would be granted the new regulator, the Federal Housing Finance Agency (FHFA). This analysis demonstrates that the supervisory authority and regulatory discretion granted the new regulator under this bill is much greater than under current law.

More...
Citigroup to Congress: Never Mind!
(Some reflections on the Gramm-Leach-Bliley Act prompted by Citigroup's exit from insurance underwriting)

Peter E. Heyward  
Venable LLP  
Washington, D.C.

There is an obvious irony in Citigroup’s decision, announced in February, to sell most of its life insurance business, thus largely completing an exit from the insurance underwriting business that began with the spin-off to shareholders of its property and casualty operations in 2002. Citigroup, as a financial conglomerate combining banking, securities and insurance in a single holding company, had been both the midwife and the most obvious beneficiary of the Gramm-Leach-Bliley Act (“GLBA”), whose enactment in 1999 (as opposed to, say, 2019) was undoubtedly hastened by The Travelers Group’s bold acquisition of Citicorp the year before. Pared down essentially to banking, securities and insurance agency activities, Citigroup could have operated under the pre-GLBA bank regulatory structure, albeit with some inconvenience.

So now that Citigroup may not really need GLBA anymore, it seems appropriate to consider what the law actually accomplished that is of lasting importance. This article is a highly selective assessment of only a few aspects of the statute, using as a framework three of the claims made for it by one of its architects, Representative Jim Leach. In his remarks at the bill signing ceremony on November 12, 1999, Congressman Leach asserted, among other things, that GLBA:

• “advances competition at home and . . . increases our ability to compete abroad;”
• “plugs the loophole that allows some mixing of commerce and banking in this country;” and
• contains “the strongest privacy provisions ever enacted into statute.”
Let’s consider each of these claims in turn.

**Competition.** The assertion that GLBA increased competition at home and abroad is in some ways the most sweeping and it can be understood to refer to many aspects of the statute. GLBA was supposed to remove artificial barriers to competition among different sectors of the financial services industry, creating a “two way street” that would allow banking organizations to engage in the securities and insurance business, while investment firms and insurance companies would be able to own banks. The banking, insurance and securities businesses were each to be functionally regulated by the appropriate federal or state regulator, under the umbrella supervision of the Federal Reserve. GLBA was also intended to provide a framework for the authorization of additional financial activities for financial holding companies, so that the law could keep pace with, rather than impede, market developments.

Measured against these lofty goals, GLBA falls short on some counts. To be sure, GLBA has been widely embraced by banking organizations. As of July 8, 2005 (the date of the most recent list on the Fed’s Web site, as of this writing) well over 600 bank holding companies in the United States (including Puerto Rico) had elected financial holding company status, the prerequisite to exercising the full range of financial powers available under GLBA. All of the 15 largest domestic banking organizations, and a substantial majority of the top 25, are financial holding companies. (Significant exceptions include credit card powerhouse MBNA Corporation – whose acquisition by Bank of America Corporation, which *is* an FHC, is pending -- and such significant regional bank holding companies as M&T Bank Corp. and North Fork Bancorp).
Thirty-seven foreign financial institutions have also elected FHC status, including, unsurprisingly, all the big Canadian banks and many, if not most, of the other non-U.S. banking organizations with a substantial U.S. presence, including Deutsche Bank, ABN AMRO, Société Générale, BNP Paribas, UBS, Crédit Suisse, HSBC Holdings and the Royal Bank of Scotland Group. No doubt the tally would be higher but for the fact that no Japanese bank holding company is an FHC, probably because the election is not yet an option for most of them, given the still-murky condition of the Japanese banking sector.

For larger banking organizations, FHC status offers significant competitive benefits:

- the ability to engage in a full range of securities powers, including running a mutual fund family, without the inconvenience of complying with the “Section 20” regime developed by the Fed while the affiliation restrictions of the Glass-Steagall Act survived;
- broader equity investment opportunities through “merchant banking” authority;
- the freedom to sell insurance without resorting to loopholes such as the “place of 5000” available to national banks, however indulgently interpreted by the forward-looking OCC;
- the flexibility to make nonbank acquisitions without Fed approval (albeit, in some cases, with a new requirement of making costly Hart-Scott-Rodino premerger filings); and
- the possibility of exercising new financial powers (should any ever be authorized).

Reportedly, the vast majority of the hundreds of smaller bank holding companies that elected to become FHCs were primarily motivated by the freedom to sell insurance that GLBA provides. It is noteworthy that the Fed’s current regulatory reform agenda
includes permitting insurance agency for bank holding companies that are not financial holding companies, and would also restore the Fed’s authority – frozen by GLBA -- to authorize new “closely related to banking” activities for non-FHC bank holding companies. If enacted, these two modest measures might prompt a number of smaller FHCs to relinquish that status.

But if GLBA swept away or lowered the barriers that had prevented or impeded affiliations among banks, securities firms and insurers, it does not seem to have induced many securities firms or insurance companies to acquire commercial banks, nor have many large banking organizations begun underwriting insurance.

It continues to be striking that few nonbank financial firms followed The Travelers’ lead in becoming bank holding companies. To date, there have been only a handful, including: The Charles Schwab Corporation (by acquiring U.S. Trust Corporation); MetLife, Inc. (by acquiring Grand Bank, N.A.); Friedman, Billings, Ramsay Group, Inc. (by acquiring FBR National Bank); Franklin Resources, Inc. (by acquiring Fiduciary Trust Company International); Countrywide Credit Industries, Inc. (by acquiring Treasury Bank, Ltd.); and Canada's Manulife Financial Corporation (by acquiring John Hancock, whose "nonbank bank" subsidiary, First Signature Bank and Trust Company, lost its exemption from the Bank Holding Company Act). None of the transactions compares in scope with Travelers/Citicorp, and several might have been possible with only modest tweaking under the pre-GLBA Bank Holding Company Act. Friedman Billings got out of the retail banking business and is no longer a bank holding company.
One can speculate as to the reasons why there has been relatively little traffic on the two-way street that GLBA was supposed to create. As recently reported in The Wall Street Journal, no doubt many bank holding companies have, like Citigroup, reached the conclusion that insurance underwriting is simply not as profitable as other banking and securities businesses.\(^1\)

As to securities and insurance companies, some would probably cite the Fed’s reputation as a strict regulator as a significant disincentive for financial firms that are not already bank holding companies to subject themselves to the Fed’s oversight, particularly when it is still possible to own a depository institution without becoming a bank holding company. While GLBA did away with the unitary thrift option (a subject that is discussed further below), it did nothing to prevent securities or insurance concerns from acquiring savings institutions. (Of the five insurance companies with banking operations named in the Wall Street Journal article referred to above, four are using thrift institutions as their banking vehicle.) The Office of Thrift Supervision, in contrast to the Federal Reserve, has been perceived as a more flexible supervisor of depository institution holding companies, and the thrift charter has many attractive features. It is well known, for example, that federally chartered thrift institutions benefit from federal preemption of burdensome state laws to at least as great an extent as national banks and also enjoy a more liberal interstate branching regime. And, in April 2001, the OTS’s Chief Counsel opined that multiple savings and loan holding companies are authorized, under the Home Owners’ Loan Act, to engage in the full range of financial activities permissible for financial holding companies under GLBA, apparently without having to meet the strict

financial and managerial criteria that apply to a bank holding company seeking financial holding company status.

The OTS has even been recognized as a consolidated supervisor by the European Union, enabling U.S. financial conglomerates that it regulates to meet the requirements of the EU’s Financial Conglomerates Directive. (It remains to be seen whether this new role will affect the OTS's relatively non-intrusive approach to holding company regulation). In sum, for financial companies willing to cope with the relatively minor and quite manageable special requirements and restrictions of the thrift charter, using a thrift subsidiary to offer insured deposit products and other banking services is eminently feasible. As discussed further regarding banking and commerce, establishing an industrial loan company is also an option for both financial and commercial or industrial companies.

The lower-than-expected traffic on the two way street may also be due to the fact that, for some players in the financial services business, sectors that had been off-limits seemed appealing for precisely that reason. Perhaps it was necessary to remove the artificial barriers for participants in the industry to take a clear-eyed look at the opportunities on the other side of the barriers, and decide that they simply were not that attractive. It is also plausible that, for some financial industry participants, the calls for a two-way street represented a tactic to forestall reform, rather than a genuine goal.

Before turning to the banking/commerce question, two additional areas where GLBA has not completely fulfilled its promise are worth a brief mention. First, functional regulation of the securities activities of banks has not been properly implemented. Although it is scarcely believable almost seven years after GLBA was
signed into law, there is still no sensible rule permitting banks to conduct certain traditional brokerage-related activities without being regulated as brokers under the Securities Act of 1934. For this, many in the banking industry would blame the SEC, which they view as seeking to achieve through regulation what it failed to gain under the carefully negotiated statutory provisions of GLBA.

A second disappointment concerns new financial powers: no significant new ones have been authorized. The Fed, in consultation with the Treasury, determined in 2000 that acting as a “finder” is an activity incidental to a financial activity, and therefore permissible for financial holding companies. The “finder” activity has long been permitted for national banks under rulings of the Comptroller of the Currency. To date, acting as a finder is the only new activity approved by the Fed under GLBA. (The Fed has also permitted all bank holding companies -- not just financial holding companies -- to conduct a broader range of nonfinancial data processing in connection with processing financial data.) Sadly (at least from the banks' perspective), a rule to permit financial holding companies to engage in real estate brokerage has been hung up by the massive opposition of real estate agents, in an effective display of the same kind of legislative lobbying that kept banks out of the insurance business for so many years. It was probably naive to hope that GLBA would put an end to such battles.

Separation of Banking and Commerce. Whether banking and commerce should continue to be separated, and if so, to what degree, was an important part of the debate regarding financial modernization that preceded the enactment of GLBA. The advocates of continued separation achieved victories in doing away with the so-called unitary thrift loophole, which had permitted industrial and commercial companies to own a single
thrift institution, and in limiting the nonfinancial activities of financial holding companies through activities such as merchant banking. Nevertheless, the claim that GLBA plugged a loophole in the separation of banking and commerce overlooks the industrial loan company option. Under a limited exemption from the Bank Holding Company Act, any kind of company can operate an ILC, a depository institution that has virtually all the powers of a commercial bank, with the exception of providing checking accounts (if the ILC has more than $100 million in assets). A number of states, including, notably, Utah, offer an ILC charter, and many industrial and commercial concerns have Utah ILC subsidiaries. In fact, Volvo, which acquired Mack Truck in 2001, owns a Utah ILC, which may be indicative of the size of this banking/commerce loophole. Whether ILCs should be permitted to offer checking accounts (or their equivalent) and enjoy expanded interstate branching options may be the next front in the banking/commerce battle.

**Privacy.** GLBA unquestionably broadened the reach of federal privacy protection to a much broader swath of companies. At the same time, it seems to have left unresolved more issues than it settled. These include:

- the degree to which federal privacy requirements should preempt state laws;
- whether opting in or out is the correct approach to information sharing with affiliates and third parties;
- the adequacy of data protection; and
- resolving the competing claims of law enforcement and personal privacy.

But it is probably unfair to fault GLBA for leaving open so many privacy-related questions. Other issues addressed by GLBA – such as the permissibility of affiliations among banks, securities firms and insurance companies, and how financial conglomerates

8
should be regulated – had been debated for years if not decades before the law was
enacted. Whatever one may think of GLBA's resolution of these issues, the advantages
and disadvantages of different approaches had been extensively considered. Privacy
questions, in contrast, had not been at the center of bank regulatory reform discussions. It
seems likely that GLBA's privacy provisions will be revisited in years to come.

* * *

Measured against some of the expectations that GLBA evoked, especially
concerning the promotion of widespread financial services firm competition under a
unified regulatory structure, the achievements of the law might seem disappointing. On
the other hand, considering how creaky the U.S. bank regulatory structure had become
with respect to affiliations among different types of financial services companies and in
other respects, GLBA – or at least significant parts of it – were both necessary and
overdue. Can anyone seriously argue that the financial services industry is not better off
under GLBA than it would be without the law? The fact that the financial services debate
has moved on to other issues is a measure of how much GLBA accomplished.

Peter Heyward would be pleased to answer questions or receive other comments
about this article. He can be reached at peheyward@venable.com.
For the past several years, legislation to reduce regulatory burden in the financial services industry has been repeatedly bogged down by a controversy involving a little known type of financial intermediary – the “Industrial Loan Company” or “ILC.” These institutions represent one of the few remaining methods by which a commercial company may own an insured depository institution, and efforts to exclude these companies from more general regulatory relief legislation has rekindled the debate over mixing banking and commerce. In part this arose from a proposal made by Wal-Mart in 2002 to charter a new ILC in California, and use this institution to provide financial services in its stores.¹ This article will review the history and current legal status of industrial loan companies.

Historical Background

Industrial loan companies or “industrial banks” were formed during the turn of the 20th Century as institutions that catered to the credit needs of low-wage industrial workers.² These early ILCs offered relatively high interest unsecured loans to factory workers who could not otherwise obtain credit. Instead of receiving deposits, these companies typically raised funds by issuing “certificates of investment” or “certificates of indebtedness.” However, Colorado and Rhode Island began to authorize ILCs to accept deposits, sometimes denoted “thrift certificates,” and the FDIC began to issue federal deposit insurance to institutions in these States as early as 1958.³ However, most ILCs were not qualified to become federally insured until the Garn-St Germain Act of 1982⁴ authorized FDIC insurance for ILCs meeting regulatory standards.

By the mid-1980s, companies engaging in non-financial activities sought to obtain control over one or more depository institutions. At that time, the Bank Holding Company Act (“BHC Act”) strictly limited the permissible activities of bank holding companies, so that companies engaging in insurance, securities underwriting, or commercial business could not own or be affiliated with a bank. However, the BHC Act narrowly defined the term “bank” to mean an institution that both: (i) accepted demand deposits and (ii) made commercial loans. To get around the BHC Act prohibition, companies formed “non-bank banks” that did not engage in both activities. For example, instead of accepting demand deposits, some of these institutions offered NOW accounts. Other non-bank banks became consumer lenders and did not make

¹ This proposal was effectively terminated by legislation in California limiting the ability of Wal-Mart to acquire a California state chartered institution.

² FDIC, “The FDIC’s Supervision of Industrial Loan Companies: A Historical Perspective” (June 25, 2004).

³ Id at 4. Between 1958 and 1979 at least six ILCs received FDIC insurance.

⁴ Public Law 97-320 (1982).
commercial loans.

**CEBA Legislation**

In response to this development, the Federal Reserve Board sought legislation to change the definition of the term “bank” to include non-bank banks. In 1987, Congress enacted a new definition of “bank” in the Competitive Equality Banking Act (CEBA), so that any FDIC-insured institution became a “bank” covered under the BHC Act. However, many exceptions were written into that law, and existing non-bank banks were grandfathered.

With respect to ILCs, the legislation created an exception for four classes of ILCs from the new definition of a “bank.” These classes are:

1. An ILC that does not accept demand deposits that the depositor may withdraw by check or similar means for payment to third parties;
2. An ILC that has less than $100 million in total assets;
3. An ILC that has not undergone a change in control after the date of enactment of CEBA (August 10, 1987), and
4. An ILC that does not, directly or through an affiliate, engage in any activity in which it was not lawfully engaged as of March 5, 1987.

With respect to classes 1 through 3, the ILC must be organized in a State that required FDIC insurance for its industrial loan companies as of March 5, 1987, or had such a proposal under consideration in the State legislature. There is no such requirement for class 4.

Any ILC that is protected by any of these provisions will lose that protection, and become a “bank” under the BHC Act, if it permits any overdraft (including an intraday overdraft) at the institution's account at a Federal Reserve Bank on behalf of an affiliate.5

It is important to recognize that these exceptions (other than class 4) do not require that the ILC be in existence as of a certain date. Thus, a new ILC can be chartered in an appropriate State at any time, and the BHC Act will not cover the institution so long as it meets one of the grounds listed above.

**Post-CEBA Developments**

---

5 However, an overdraft that results from an inadvertent computer or accounting error that is beyond the control of the ILC and the affiliate is excused, as well as an overdraft on behalf of an affiliate in connection with activities that are financial in nature (and that does not violate sections 23A or 23B of the Federal Reserve Act). 12 U.S.C. § 1841(2)(H).
As noted previously, most ILCs are authorized to engage in traditional financial activities that are available to all charter types. They make all kinds of consumer and commercial loans and may accept federally insured deposits. They may be original issuers of Visa or MasterCard credit and debit cards and may fund their operations with Federal Home Loan Bank borrowings. An ILC may be organized as a limited-purpose or credit-card institution, and thus limit its products and services to those specified by its charter.

ILCs are subject to the same regulatory and supervisory oversight (including the laws and regulations pertaining to bank safety and soundness and consumer protection) as other State-chartered banks, except for the BHC Act and the Federal Reserve Board’s supervisory authority over companies that own or control “banks.” This exemption from the BHC Act is very troubling to the Federal Reserve Board. The Board’s position is that “allowing a commercial or financial firm to operate an insured nationwide bank outside the supervisory framework established by Congress for the other owners of insured banks raises significant safety and soundness concerns, creates an unlevel competitive playing field, and undermines the policy of separating banking and commerce that Congress reaffirmed in the Gramm-Leach-Bliley Act of 1999.”

On the other hand, the flexibility of the ILC charter and its exemption from holding company regulation has made this type of institution an attractive choice for companies that are not permitted to, or choose not to, become subject to the restrictions of the BHC Act. As a result, it is not surprising that the parent companies of ILCs include a diverse group of commercial firms.  

**Legislative Proposals – the Gilmore-Frank Amendment**

The ILC exemption from the definition of a “bank” under the BHC Act has been raised recently in connection with regulatory reform proposals, as well as with legislation to permit the payment of interest on checking accounts and Federal Reserve required reserves. Last year, H.R. 1375, as passed by the House of Representatives contained language known as the “Gilmore-Frank” amendment. This provision was also included in the legislation recently passed by the House of Representatives to permit commercial banks to pay interest on checking accounts.

Under the Gilmore-Frank provision, the benefits of the legislation will not apply to any ILC that is owned by a parent company that receives 15 percent or more of its annual gross revenues from non-financial activities. However, this restriction will not apply to:

(I) An ILC that became insured before October 1, 2003 or pursuant to an

---


7 Section 401(b)(2) of H.R. 1375.

8 H.R. 1224, passed by the House on May 24, 2005.
application for insurance what was approved by the FDIC before that
date; and

(II) There was no change in control of the ILC after September 30, 2003.

Conclusion

Industrial loan companies remain as one of the few types of FDIC-insured
depository institutions that are not subject to the BHC Act. As such, they are
attractive vehicles for non-financial companies seeking to own or control a bank.
However, ILCs must conform to certain restrictions in order to retain their
exemption from the BHC Act. In addition, recent activity indicates that the
Federal Reserve Board has strong views that these institutions should be limited,
and some in Congress have taken the position that ILCs should not get the
legislative benefits that would be provided to depository institutions under recent
legislative proposals.

Ray Natter would be pleased to answer any additional questions you may
have regarding industrial loan companies. He may be reached at rnatter@barnett-
sivon.com.
Information Security: Principles and Best Practices
by
Thomas P. Vartanian, Mark Fajfar and Robert H. Ledig
Fried, Frank, Harris, Shriver & Jacobson LLP
July 14, 2005

Ever easier access to electronic information systems has fueled an explosion of new products and services available at remote locations via the Internet. Sophisticated transactions are no longer confined to the back office. This dependence on remote access to electronic information systems requires a compromise between accessibility and security, since the very process of making a system widely accessible will lessen its security. From a legal perspective, information security principles and best practices are discerned from regulatory guidance and legal precedents as to the proper course to follow in counteracting information security threats.

What Are the Threats to Information Security?

Just as information systems have a near pervasive presence in the business and financial world, a wide variety of sources pose threats to information security. The key source of vulnerability, however, is the increasing reliance on remote interaction. Rather than being centralized, transactions occur at various remote terminals or via the Internet, and are often completed solely by the consumer. This reliance on remote, decentralized interaction, with a variety of innovative products and services available, is also the characteristic which renders information systems vulnerable to fraud, hacking and other disruptions.

To understand these threats, it is helpful to classify them in four broad categories:

- Unauthorized access to personal information stored on a system in order to perpetrate identity theft.
- Unauthorized access in order to steal information or assets maintained on that system.
- Corruption of data, as vandalism or extortion of the organization that maintains the system.
- Unauthorized access or use in order to mask illegitimate or illegal transactions – e.g., money laundering.

Recently, several information security breaches of the first type have drawn wide attention – most notably, incidents involving unauthorized access to files maintained by ChoicePoint, Inc. and credit card information stored by CardSystems Solutions Inc. This type of
breach has also engendered litigation, such as the pending lawsuit *Pennsylvania State Employees Credit Union v. Fifth Third Bank*, 1:04-cv-01554-WWC (M.D. Pa. 2004), which involves a breach of the systems of BJ’s Wholesale Club. Examples of the other types of breaches include *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001), where the defendant hacked into and threatened to disable the systems of an e-commerce business unless a ransom was paid.

**Information Security Standards**

To guide the response to these threats, a variety of government and non-government organizations have developed legal requirements and other standards of varying scope. All or some of these standards may be applicable to any particular situation.


- In the non-financial area, the Department of Health and Human Services, for example, has promulgated Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164.302 et. seq. under the Health Insurance Portability and Accountability Act (“HIPAA”).

- The Sarbanes-Oxley Act and implementing regulations promulgated by the Securities & Exchange Commission regarding internal controls require the monitoring of information systems.

- The National Strategy to Secure Cyberspace, promulgated by the President pursuant to the Federal Information Security Management Act (“FISMA”) and Executive Order 13231.

- Court opinions have delineated the requirements of due care with regard to information security in a wide variety of particular situations.

- Accounting standards and standard-setting bodies, such as SAS 70, CobiT, and COSO are applicable to information security

- Private financial networks such as the credit card networks, the ATM networks and check-clearing systems impose information security standards.

- There is a developing information security common body of knowledge set forth in standards such as ISO 17799 and the Generally Accepted Information Security Principles (“GAISP”).
Adding to the complexity, these various information security standards are subject to nuanced interpretation. Which legal standard will apply may depend both on the type of business (e.g., only financial institutions are covered by certain information security requirements of the GLBA) and the type of data (e.g., “protected health information” as defined in HIPAA) that is involved. The regulators which interpret the standards provide “guidance,” not black and white rules. The accounting standards and private network rules depend on interpretation by private parties, which may not always be publicly available. Lastly, although new cases appear with increasing frequency, a general scarcity of legal precedents exists due in part to reluctance to publicly report information security breaches or settlements.

Steps to Information Security Compliance

Obviously, sophisticated electronic systems and technical procedures exist which can be used to secure information systems. From a legal perspective, however, the primary areas of concern are not the technical details, but the measures taken at a systemic level to protect information systems. Lawyers view the security system as a whole, in order to prepare for an eventual review or examination by a third party, such as a regulator, an independent auditor, an adverse party in litigation, or an internal investigation conducted by the organization itself. (See, for example, Section 341, “Technology Risk Controls,” of the Regulatory Handbook issued by the Office of Thrift Supervision.)

What compliance steps are required to meet legal and regulatory standards for information systems? The following checklist is gleaned from pronouncements and guidance issued by, among others, the federal banking regulators and the Federal Trade Commission.

- **Security efforts must reflect top-level consideration.** The board of directors must lay down guiding information security principles and see to their enforcement throughout the organization.

- **Security efforts must be “risk-based.”** meaning that one must evaluate threats and concentrate on counteracting those that involve the highest risk of severe adverse consequences.

- **Security efforts must be continuous.** Compliance measures must be periodically tested, reevaluated and modified to maintain their effectiveness as the organization’s activities evolve.

- **Security efforts must cover the entire system.** Specific practices and the compliance culture must be overseen by the board of directors and extend to the lowest level of employee with operational responsibility.
• **Information systems must permit later auditing in order to detect efforts to alter or compromise information.** Just as the “black box” is crucial to the investigation of a plane accident, there must be some means of reviewing how the information systems have actually been used and what they have actually done.

• **Third-party service providers must be held to high standards.** When information systems tasks are subcontracted (or “outsourced”) to third party service providers, responsibility for information security cannot also be delegated. On the contrary, these arrangements require close attention to the subcontractor’s performance.

**Manage Information Security as Part of Overall Legal Compliance**

Most important, the goal is not to create a list of compliance steps, and then conclude that if each of those actions is completed, the information system will be sufficiently secure. Instead, information security must be a part of the organization’s overall legal compliance effort. For example, decisions about specific hardware or software measures need to be made and documented methodically, so that when the security of the system is later examined by a regulator or third-party, the organization will be able to explain why it took the steps that it did, and did not take other steps. Similarly, it is important to maintain access controls and logs, so that it is possible to examine how the system is used – to understand, for example, how a security breach occurred, to what extent information was compromised, and so forth.

**Adverse Consequences of Information Security Lapses**

An information security lapse can lead to substantial financial liability. An organization that does not protect the information entrusted to it may be subject to fines or other penalties imposed by regulators, and to the costs of class-action lawsuits which, in addition to any eventual judgment, may be expensive to litigate or settle. (See, for example, the wide variety of claims made in *Harrington v. ChoicePoint*, No. 2:05-CV-01294-MRP-JWJ (C.D. Calif., filed Feb. 22, 2005).) Information security errors can also lead to high remediation costs (such as refunds to improperly billed customers), and a history of such errors may lead to increased insurance costs.

Information security steps are also necessary in order to fulfill corporate governance responsibilities. The Sarbanes-Oxley Act and its implementing regulations require internal controls to monitor whether a company’s information systems are operating properly. And, a
company’s disclosure regarding risks to its information systems must keep pace with its ever increasing reliance on those systems.

Needless to say that while the use of electronic technology has increased the range of financial choices for consumers, it has also rendered every business vulnerable to increased reputational risk. For this reason, information security is a critical element in maintaining consumer confidence. If customer information is disclosed or stolen and used improperly in an identity theft scheme, the company is likely to face not only possible liability for amounts stolen in the scheme, but also a strong customer backlash, given the sensitivity to this risk. The recent parade of regulators and businesses testifying about identity theft before the Senate Banking Committee, the Senate Committee on Commerce, Science & Transportation and the House Financial Services Committee, among others, are only one example of the consequences of focused public attention on the pervasive business use of information systems, and the vulnerability of those systems.

Cost / Benefit Analysis

To select the particular preventive measures to be adopted in order to put regulatory “best practices” into effect, a cost/benefit analysis has long been recognized as a useful tool. In the seminal case The T.J. Hooper, 60 F.2d 737 (2d Cir. 1932), the court held that when technology that could have prevented an accident is available and not overly costly, the failure to implement that technology can be the basis for legal liability. The implications for information security are clear – if a security measure passes a cost / benefit analysis, one may be held legally responsible if it is not implemented.

For further information on these topics or the regulations and standards discussed above, please feel free to contact the authors by email at 21stCen@friedfrank.com.
Banking Agencies Issue Guidance on Response Programs for Unauthorized Access to Customer Information

Charlotte M. Bahin
Senior Vice President, Regulatory Affairs,
America’s Community Bankers

Introduction

With increased frequency, the confidential personal information of customers of various entities has been compromised. Generally, the breaches to date have not involved an insured institution directly, but have resulted from an action or inaction of a third party. Nonetheless, in several well-publicized situations, it is the financial institution with which many customers have contact and to whom they look to for recourse.

In 2003, the federal banking agencies issued a proposal that would interpret Section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act") and supplement the Interagency Guidelines Establishing Information Security Standards (Security Guidelines). This interpretation and supplement is the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (final guidance). The final guidance establishes a risk-based framework for financial institutions to develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider.

Given the nature of relationships that insured depository and other financial institutions have with their customers and the types of information that they and their service providers retain about customers, the development of a plan to respond to security breaches is among the most important plans to have in place. Like many requirements of the agencies, the plan must be risk-based so a noncomplex institution with few relationships with third parties will have a relatively simple plan but the more complex the organization and the more parties involved, the more detailed a plan is necessary. The enormous risk to the reputation of the institution for a breach of security is only compounded by not having a plan in place for responding to customers and regulators.

The issuance of the final guidance by the federal banking agencies has highlighted for Congress and many state legislatures the need for legislation in this area. While many states have recognized exceptions in their legislation for insured depository institutions on account of the Security Guidelines, not all states have done so. As the debate continues, therefore, insured institutions are in a better position than other types of companies, in particular, if federal legislation preempts state law. However, it will be important for the industry to comply with the requirements already imposed to maximize this position.

---

1 70 Fed. Reg 15736 (March 29, 2005)
2 Public Law 106-102
General Requirements

The GLB Act requires the agencies to establish standards for institutions within their jurisdiction that include administrative, technical, and physical safeguards to protect the security and confidentiality of customer’s information. The Security Guidelines require financial institutions to have a program that:

- Ensures the security and confidentiality of customer information;
- Protects against any anticipated threats or hazards to the security or integrity of such information; and protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The Security Guidelines issued to implement Section 501(b) direct financial institutions to assess the following risks when developing a program:

- 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; and
- Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

The final guidance requires every financial institution to have a response program designed to address incidents of unauthorized access to customer information maintained by the institution or its service provider. The particular program must be designed with the operations, size, complexity and specific risks identified for the specific institution.

Who and What is Covered by the Guidance

The agencies have clarified that the final guidance contains the same scope and identical definitions as are found in the Security Guidelines, which are generally the same as those in the agencies privacy rules also required by Title V of the GLB Act. For example, “customer information” means any record containing nonpublic, personal information about a customer, whether in paper, electronic, or other form, maintained by or on behalf of the institution. The final guidance is applicable only to information that is within the control of the institution and its service providers, and does not apply to information that is disclosed directly by the consumer to a third party, for example through a fraudulent website.

The final guidance is applicable to a wide range of financial institutions and subsidiaries, except those entities that are under the jurisdiction of another federal regulator. While the guidance does not apply to a financial institution’s foreign offices, branches, or affiliates, financial institutions are responsible for the security of its customer information whether
the information is maintained within or outside the United States, for example by a service provider located outside the United States.

Finally, the final guidance does not apply to information involving business or commercial accounts. The term “customer” means a consumer who obtains a financial product or service from a financial institution to be used primarily for personal, household, or family purposes and who has a continuing relationship with the institution.

The Response Program

The agencies clarify that a response program should be an integral part of an institution’s information security program. A financial institution should implement those security measures designed to prevent unauthorized access to or the use of customer information. Examples of actions include placing access controls on customer information systems and conducting background checks on employees who are authorized to access customer information. Each institution should develop and implement security measures designed to address incidents of unauthorized access to customer information that occur despite measures to prevent security breaches.

Service Provider Contracts

Given the increasing number of arrangements that banks have with third parties that may have access to personal information of the customers of the institution, the contract with the service provider must contain a number of provisions. The contract should require the service provider to address incidents of unauthorized access to the institution’s customer information, including by notifying the institution as soon as possible of any breach so that the institution may implement its response program as quickly as possible.

The final guidance does not provide a grandfather for existing contracts or a transition period for existing contracts to come into compliance, because the agencies believe the final guidance is an interpretation of the Security Guidelines which are already in effect. Contracts that are not in compliance should be amended as soon as possible. The final guidance also clarifies that a financial institution should be able to address incidents of unauthorized access to customer information in information systems maintained by both domestic and foreign service providers.

Components of a Response Program

The program must be risk-based and reflect the nature and complexity of the institution. The agencies determined that the final guidance should provide flexibility to financial institutions in the drafting and implementation of their plans. The final guidance itself does not include much detail about the elements of the plans. The minimum elements of the plan should include procedures for:

- Assessing the nature and scope of an incident, and identifying what customer information systems and types of information have been accessed or misused;
• Notifying its primary federal regulator as soon as possible when the institution becomes aware of the incident involving unauthorized access to or use of sensitive information;
• Immediately notifying law enforcement in situations involving federal criminal violations requiring immediate attention, consistent with the requirements to file Suspicious Activity Reports;
• Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and
• Notifying customers when warranted.

Standard for Notice to Regulators

The final guidance provides that the standard to be used to determine whether and when notice should be given the primary federal regulator is that as soon as possible when an institution becomes aware of an incident involving unauthorized access to or use of “sensitive customer information.” The definition of sensitive customer information is defined to mean a customer’s name, address, or telephone number in conjunction with the customer’s social security number, driver’s license number, account number, credit or debit card number or e personal identification number or password that would permit access to the customer’s account. The term also means any combination of components that would allow someone to log onto or access the customer’s account such as a user name or password and account number.

The final guidance also provided that it is the responsibility of the financial institution not the service provider to notify the regulatory of any intrusion. However, a financial institution may contract with a service provider or may authorize a service provider to notify the regulator when a security breach involves an unauthorized intrusion into the institution’s customer information systems maintained by the service provider.

Customer Notice

One of the most important practical elements of the an institution’s plan is when and how to notify its customers. When and how this notice is given can minimize or increase the reputation risk and the legal liability for an institution whose customer information has been compromised. The guidance describes whose responsibility it is to provide notice and what the standard should be. The timing of the notice is also addressed.

The final guidance states that institutions have an affirmative duty to protect their customer’s information from unauthorized use or access. Management of the institution’s reputation and legal risk can be accomplished at least in part by providing timely notice. The final guidance specifically states that when customer notification of an incident is warranted, the institution may not forgo notifying customers because of potential embarrassment or inconvenience.
When the institution becomes aware of a breach, it must conduct a reasonable investigation to determine the likelihood that sensitive customer’s information has been or will be misused. If the determination is that misuse of such information has occurred or may reasonably occur, the institution should notify the customer as soon as possible. Such a customer notice may be delayed if law enforcement determines that a notice will interfere with a criminal investigation.

The customer notice must be given in a clear and conspicuous manner. It should describe the incident in general terms and describe any actions taken to prevent further unauthorized access to the information. The notice should remind the customer to remain vigilant and report incidences of identity theft to the institution. Any notice must be sent in a manner designed to reasonably ensure that the customer will receive it.

For more information or questions about this article, please contact Charlotte Bahin at (202) 857-3121 or cbahin@acbankers.org.
On May 25, 2005, the Financial Services Committee of the U.S. House of Representatives overwhelmingly approved a bill, H.R. 1461, to strengthen the supervision and regulation of Fannie Mae and Freddie Mac (the “GSEs” or the “Enterprises”). The bill has engendered some controversy based, in part, on provisions that could be used to enhance the GSE’s competitive position, such as increases in the size of loans that Fannie Mae and Freddie Mac can purchase. Arguments have also been made that the regulatory and safety and soundness provisions in the bill are too weak, and that these areas of the bill are “worse than current law.” This article will address this second point only, and will compare the regulatory and safety and soundness authority of the GSE’s current regulator, the Office of Federal Housing Enterprise Oversight (OFHEO) with the authority that would be granted the new regulator, the Federal Housing Finance Agency (FHFA). This analysis demonstrates that the supervisory authority and regulatory discretion granted the new regulator under this bill is much greater than under current law.

Regulatory Independence

Under current law, OFHEO’s independence is circumscribed. Unlike the Federal banking agencies, OFHEO does not have independent litigating authority, and the agency must ask the Justice Department to argue its cases in court, and even to enforce its subpoenas. The agency’s budget is subject to the Congressional appropriations process, despite the fact that funds are raised through assessments on the GSEs and not appropriations. The agency’s authority over the GSEs does not extend to the housing mission, and thus approval of new programs for the Enterprises rests with the Secretary of HUD, and not OFHEO.

The bill, on the other hand, provides the regulator with much of the independence that the banking agencies currently enjoy. The Director of the FHFA is given a five-year term and may be removed only for cause. Congressional testimony does not have to be cleared by the Administration, and funding is independent of Congressional appropriations. The agency has independent litigating authority and would no longer be dependent upon the Justice Department to enforce safety and soundness related subpoenas. The regulatory role of the Secretary of

---

5 H.R. 1461 § 101 (All references to H.R. 1461 are to the committee passed bill).
6 H.R. 1461 § 102(b).
7 H.R. 1461 § 106.
8 H.R. 1461 § 102.
HUD would be eliminated, and the new agency would have responsibilities for all activities of
the GSEs.

On the other hand, the bill also contains a provision that goes against independence. This
is the section that creates an Oversight Board that includes the Director of FHFA, the Secretaries
of the Treasury and HUD, and two Presidentially appointed members. While this Board is not
given any regulatory authority, it is authorized to have a permanent staff, and could assume a
prominent role in the overall direction of the agency. However, even with this provision, the
new agency would have considerably more independence from political influence than at
present.

Activity and Program Approval Authority

Under current law, the GSEs must submit a proposal to engage in a “new program” to the
Secretary of HUD, who may take up to 60-days to review the proposal. If the Secretary does not
act within this period, the new program is deemed approved. The term “new program” is
defined as a significantly different program for dealing in conventional mortgages. There is no
explicit authority for the Secretary to review other activities of the Enterprises.

The bill requires that both new programs and new business activities be submitted to the
Director of FHFA for prior approval. The Director must publish “new program” proposals in
the Federal Register and solicit public comment. Proposals for new business activities are not
published in the Register, but the Director is given 30-days to reject the new activity. The bill
also gives the Director authority to declare almost any GSE activity to be a “new activity,” and
make it subject to prior review procedures. If the Director determines that any activity the GSE
is engaging in “consists of, relates to, or involves” a new business activity, the Director may
prohibit the activity until it is submitted for review. The bill also contains a provision that may
allow the Director of FHFA to issue a “conditional approval” at any time. This provides the
Director additional discretion to expedite an approval, and perhaps even waive the publication
requirements. This provision adds to the Director’s regulatory discretion, it does not in any way
diminish his or her authority.

These provisions are important enhancements over the current statutory language, and
clearly allows the FHFA to review proposed business activities, and if appropriate, to deny the
proposed activity or program based on safety and soundness, the underlying statutory purposes
for the GSEs, or the “public interest.”

---

9 H.R. 1461 § 103.
12 H.R. 1461 § 122.
13 Id.
14 Id.
On-Going Activity and Program Review

Even if an activity or program is approved, the bill gives the Director of FHFA new authority to determine that the GSE must modify the activity or program, or cease from engaging in the activity, based on safety or soundness concerns, or a finding that the activity is inconsistent with the authorizing Acts.

The Director’s authority in this regard is quite broad and specific. The Director must conduct a periodic review of all of the assets and liabilities of the GSEs and may order the Enterprise to dispose of any asset or liability. For example, since the purpose of the GSE is to foster liquid and efficient housing finance markets, the Director could determine that a GSE must divest itself of non-housing assets, such as automobile loans. This is an important and significant clarification of the Government’s authority to require divestiture of non-mission related assets.

Prudential Management and Operations Standards

Unlike the banking agencies, OFHEO has no explicit statutory authority to issue mandatory prudential management and operations standards. The agency has instead used its general regulatory authority to issue such standards. The legislation provides the explicit statutory basis for such standards, and mandates that the standards include portfolio management, credit and counterparty risk, internal controls, internal audit, market risk, the issuance of subordinated debt, records maintenance, and similar items. Failure to comply with a standard may result in higher capital requirements, limitation on growth, or other remedial actions by the FHFA.

Capital and Prompt Corrective Action

Currently, OFHEO has limited ability to set capital levels. Essentially, these levels are dictated by statute. The bill, on the other hand, gives the Director of the FHFA complete discretion to set capital levels by regulation, and if necessary, to require additional capital based on the activities or programs of a particular GSE. The Director may also order a GSE to make a temporary adjustment to capital if the GSE is engaging in certain unsafe or unsound practices, is deemed to be in an unsafe or unsound condition, or violates any operational or management standards that must be established by the Director. Finally, the legislation provides the Director essentially the same tools as the Federal banking agencies to take significantly more stringent “prompt corrective actions” as the capital level of a GSE falls below the adequately capitalized level.

---

15 H.R. 1461 § 113.
16 H.R. 1461 § 102.
18 H.R. 1461 §§ 111, 112.
19 H.R. 1461 § § 4614 et. seq.
Enforcement Powers

The current scope of OFHEO’s enforcement powers is limited, and for example, the agency lacks explicit authority to take action against many “enterprise affiliated” parties that might be involved in malfeasance at the GSE.\(^{20}\) Also, OFHEO has no specific statutory authority to remove a bad actor from a GSE. The bill addresses these issues, and provides the Director with explicit enforcement powers that are similar to those of the Federal banking agencies. For example, under the bill, a violation of any law may serve as a basis for an enforcement order.\(^{21}\) Further, the FHFA is given jurisdiction over any party participating in the affairs of the Enterprise.\(^{22}\) Civil money penalties are also increased. The maximum penalty that may be assessed against an Enterprise is set at $2 million per day, per violation.\(^{23}\) Even for a GSE, an annualized penalty of $730 million per violation would certainly motivate the board of directors, if not the executives, to take corrective action.

Conservatorship and Receivership

OFHEO currently has the authority to place an Enterprise into a conservatorship, but does not have the power to place a GSE into receivership. The bill gives the Director of the FHFA the same authority to place a GSE into a conservatorship or receivership as the banking agencies have with respect to banks.\(^{24}\)

Conclusion

H.R. 1461, as passed by the House Committee on Financial Services, provides the new GSE regulatory agency, the FHFA, with explicit and enhanced authority in the areas of general regulatory power, safety and soundness tools (including prompt corrective action powers), capital, program and activity review, enforcement and removal powers, independent litigating authority, and receivership. These provisions provide FHFA with considerably more authority to take various remedial actions than currently provided to OFHEO, and considerably more discretion in regulating and supervising the GSEs. Other provisions in the bill, including those that relate to the competitive position of the GSEs or their responsibilities to provide for more affordable housing for low- and moderate-income families are beyond the scope of this brief review.

\(^{21}\) H.R. 1461 §§ 161.
\(^{22}\) H.R. 1461 § 2.
\(^{23}\) H.R. 1461 § 165.
\(^{24}\) H.R. 1461 § 144.