

## Financial Institutions

[www.schiffhardin.com](http://www.schiffhardin.com)

**Darren C. Baker**

312.258.5538  
dbaker@schiffhardin.com

**Lorraine M. Buerger**

312.258.5837  
lbuerger@schiffhardin.com

**Matthew Galo**

312.258.5643  
mgalo@schiffhardin.com

**David S. McCarthy**

312.258.5653  
dmccarthy@schiffhardin.com

**Gary L. Mowder**

312.258.5514  
gmowder@schiffhardin.com

**Harold S. Nathan**

212.745.0813  
hnathan@schiffhardin.com

**Peter L. Rossiter**

*Client Service Group Leader*  
312.258.5579  
prossiter@schiffhardin.com

**John Schietinger**

312.258.5817  
jschietinger@schiffhardin.com

**David H. Williams**

404.437.7010  
dwilliams@schiffhardin.com

**Jason L. Zgliniec**

312.258.5795  
jzginiec@schiffhardin.com

To Our Clients and Friends:

We are pleased to bring you another edition of Schiff Hardin's *Financial Institutions Update*.

These are the most tumultuous times for the financial services industry and the interconnected global economy that anyone active in the industry today has ever seen. It's impossible to do these fast-moving developments justice in a publication like this, and we won't try. (See page 19 for a description of our Financial Crisis Team.) But other parts of life go on, and all of us need to stay current on regulatory, accounting and other developments. That's the role of the *Financial Institutions Update*.

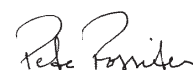
In this edition, we have an excellent piece by **Jeff Ellis**, Managing Director with Huron Consulting, on the new rules for business combination accounting about to come into force. They will change how all M&A transactions in financial services are booked and are well worth your attention.

We also bring you a "Regulatory Roundup," covering a number of new or changed regulatory requirements that are in the proposal stage, recently became law or are about to come into force – the Affiliate Marketing Rules; the Red Flag Rules; Regulation R; Regulation Z Amendments; and the ever-popular Basel II Capital Rules, which may now be available to all banks, not just the largest.

Data security issues show up in the news just about every week. **Darren Baker** summarizes the federal guidelines for dealing with security breaches that apply to banks. **Charlene Kalebic** covers another set of rules that may be less familiar to bankers but are no less important – the state rules, adopted in 40-some states.

**Lori Buerger** contributes a piece on "covered bonds," a new way of dealing with mortgage financing that looked like it was getting traction until the present turmoil stopped many developments in their tracks. It still may prove to be part of the way out of the woods.

So take a break from the headlines and catch up with these developments. Who would have thought that the normal flow of regulatory change could be soothing?



**Pete Rossiter**

# Accounting for Business Combinations: Changes Expected to Result in Increased Volatility of Earnings

by Jeffrey H. Ellis

Managing Director, Huron Consulting Group

With the world's financial markets in turmoil, how to account for business combinations may be about the last thing going through the minds of most bankers. However, the credit crisis will present opportunities for stronger financial institutions and commercial companies to make strategic and selective acquisitions. Therefore, it is important to understand the impact on an acquiring company's financial statements of some of the more significant changes made by the Financial Accounting Standards Board ("FASB") in Statement of Financial Accounting Standards No. 141 (revised 2007), *Business Combinations* ("SFAS 141R"). Financial institutions, as users of financial statements in making credit decisions and monitoring borrowers' financial performance and as potential acquirers in transactions that will be subject to SFAS 141R, will need to understand the effects of the new standard. This article highlights some of the more significant changes from SFAS 141, *Business Combinations*.

## Introduction

The FASB issued SFAS 141R in December 2007. SFAS 141R applies to all business combinations for which the acquisition date (the date on which the acquirer gains control of the target) is on or after the beginning of the acquirer's fiscal year beginning on or after December 15, 2008 (in English, SFAS 141R is effective for companies with a calendar year end for transactions consummated on or after January 1, 2009). SFAS 141R requires an acquirer to recognize the assets acquired and liabilities assumed of a target company at fair value, and requires companies to apply the guidance in SFAS 157, *Fair Value Measurements*, a much-maligned standard that some blame (incorrectly) for the credit crisis, to determine the fair value of those assets and liabilities. Because SFAS 141R requires fair value measurements for many non-financial assets and liabilities not currently recorded at fair value, it is likely that implementation issues will arise as valuation professionals begin to attempt to estimate fair values for those assets and liabilities. Preparers, auditors and users have raised many issues with the FASB's Valuation Resource Group since its formation last year in anticipation of some of those implementation issues.

## Definition of a business

SFAS 141R defines a business more broadly than SFAS 141. Therefore, it is likely that more asset acquisitions will qualify as business combinations. Under SFAS 141, an integrated set of activities and assets had to be self-sustaining and conducted and managed to generate a return to investors. Under SFAS 141R, the integrated set of activities and assets does not need to be self-sustaining, and only needs to be capable of being conducted and managed to generate a return. This change has the potential to significantly impact the purchase price assigned to assets acquired and liabilities assumed and the post-combination results of operations because of the differences between accounting for asset acquisitions and business combinations under SFAS 141R.

As creditors, financial institutions should expect to see an increase in transactions that companies account for as business combinations. For example, acquisitions of power plants, office buildings, and hotels will likely meet the revised definition of a business. Similarly, to the extent not already considered businesses, financial institutions should expect to account for the acquisition of branches as business combinations.

### Measuring the consideration paid in an acquisition

Under SFAS 141, a company that issues its common stock as consideration in a business combination measures the fair value of the stock based on the price a few days before and a few days after the announcement. SFAS 141R will require an acquirer to determine the fair value of its stock at the acquisition date. Accordingly, changes in the acquiring company's stock price in the interim between the announcement and the acquisition dates will directly affect the purchase price allocated to assets acquired and liabilities assumed.

### Determining the cost of the target business

In addition to changing when an acquirer measures the fair value of its common stock, SFAS 141R precludes an acquirer from including transaction costs as part of the cost of the acquired business, but requires the acquirer to include an estimate of the fair value of any contingent consideration arrangements as part of that cost.

*Transaction costs* – Under current practice, companies include transaction costs (including advisory, legal, accounting and valuation services) incurred in acquiring the target company as part of the purchase price. Because SFAS 157 does not consider transaction costs part of the fair value of an asset acquired, SFAS 141R will require companies to expense costs paid to third parties in connection with a business combination as it incurs those costs. That change will reduce an acquiring company's pre-combination earnings and the amount of goodwill reported in an acquisition. It will also make it more difficult for a public company to keep hidden potential acquisitions that come together over an extended period because it will be required to explain changes in expenses in its quarterly filings with the SEC. The change may also cause a company to look more closely at the fees it is paying to its advisors, recognizing that those fees will now directly affect the company's earnings.

*Contingent consideration* – SFAS 141R will require the acquirer to include an estimate of the fair value of a contingent consideration arrangement as part of the purchase price of a target company. It will also require the acquirer to classify that arrangement as either a liability or equity based on the guidance in other FASB standards (such as SFAS 150, *Accounting for Certain Financial Instruments with Characteristics of both Liabilities and Equity*). If the arrangement does not qualify as equity, the acquirer will be required to mark the arrangement to fair value until the contingency is resolved, which could significantly increase the volatility of post-combination earnings. For example, if the acquirer agreed to issue to the selling shareholders additional shares with a fair value of \$25 million if the target company achieves specified goals, the acquirer would account for the contingent consideration arrangement as a liability. The acquirer would recognize subsequent changes in the fair value of the arrangement in earnings.

## Adjustments to loan losses

SFAS 141R requires a company to record assets acquired and liabilities assumed at their acquisition date fair values. For loans and receivables, an acquirer will not only need to consider current interest rates at the acquisition date (as currently required by SFAS 141), but will also need to consider credit risk in estimating the fair value of the acquired loans and receivables. Although the SEC staff has not retracted the guidance in Staff Accounting Bulletin (“SAB”) 61, *Adjustments to Allowances for Loan Losses in Connection with Business Combinations*, the guidance in SAB 61 to carry forward the allowance recorded by the target company is inconsistent with the requirements in SFAS 141R. The target company will have applied SFAS 5, *Accounting for Contingencies*, and SFAS 114, *Accounting by Creditors for Impairment of a Loan*, both of which preclude a company from recognizing an allowance when it is not probable that a loss has been incurred or the amount of the loss is not reasonably estimable, to determine the loan loss allowance. These thresholds for recognizing a loss in SFAS 5 and SFAS 114 are inconsistent with a fair value measurement, where loss probability and ability to estimate the loss are simply factors in estimating the loss. This change will impact any ratios based on the allowance disclosed by a financial institution, and may also impact the amount of the allowance that can be added back for purposes of determining regulatory capital.

## Contingencies

SFAS 141R significantly changes the accounting for preacquisition contingencies. It requires the acquirer to determine if the contingency is contractual or non-contractual. An acquirer is required to recognize an asset or liability for the acquisition date fair value of contractual contingencies. For non-contractual contingencies, SFAS 141R will require the acquirer to determine if it is more likely than not that the contingency gives rise to an asset or liability and, if so, the acquirer is required to recognize an asset or liability for the fair value of the contingency.

One area in particular that may cause difficulties for companies is the accounting for non-contractual contingent liabilities arising from litigation. In determining whether it is more likely than not the company has incurred a liability for a particular matter, the acquirer considers only the merits of the case; its intent to settle the case is not relevant to the more likely than not conclusion. If the acquirer concludes that it is not more likely than not the litigation gives rise to a liability, SFAS 141R precludes the acquirer from recognizing a liability in purchase accounting, even if it concludes that a loss is probable under SFAS 5 because it intends to settle the litigation. This issue may be particularly important to financial institution acquisitions arising out of the credit crisis. Because of concerns raised by the legal community over privilege and prejudicial information, the FASB decided at its October 29, 2008 meeting to propose an amendment to SFAS 141R’s guidance on preacquisition contingencies. The amended guidance, if adopted, would eliminate the distinction between contractual and non-contractual contingencies and would instead require an acquirer to recognize an asset or liability arising from a contingency if it can reasonably estimate the fair value. Based on the discussion at the FASB meeting on when fair value is reasonably estimable, it appears the amended guidance would permit an acquirer to recognize a liability in purchase accounting for litigation it intends to settle. It is not clear, however, that the amended guidance will resolve concerns over privilege and prejudicial information.

The above list of differences between SFAS 141 and SFAS 141R is not all-inclusive; there are many other important differences between the accounting under those two standards. Although not addressed in this article, financial institutions should also be aware of the differences between SFAS 141R and International Financial Reporting Standard (“IFRS”) 3, *Business Combinations*, particularly given what appears to be an inevitable move to IFRS in the near future.

---

Jeffrey H. Ellis is a member of Huron’s Accounting & Financial Consulting Practice and is the leader of the complex accounting team. He can be reached at 312.880.3019, or at [jellis@huronconsultinggroup.com](mailto:jellis@huronconsultinggroup.com).

Huron’s Accounting & Financial Consulting Practice assists corporations with complex accounting and financial reporting matters, financial analysis in business disputes and litigation, as well as valuation analysis related to complex financial instruments and business acquisitions. It is comprised of certified public accountants, economists, certified fraud examiners and valuation experts that serve attorneys and corporations as expert witnesses and consultants in connection with business disputes, as well as in regulatory or internal investigations.

## Regulatory Roundup

The bank regulatory agencies’ focus on credit quality in light of the current strains in the economy and financial markets has not resulted in any let-up on other regulatory fronts. Here are some recent developments of interest.

### Affiliate Marketing Rules

On October 25, 2007, the Federal Trade Commission (the “FTC”) and the federal financial regulatory agencies published final rules governing the use of consumer information received from affiliates for marketing purposes (the “Affiliate Marketing Rules”), implementing Section 214 of the Fair and Accurate Credit Transactions Act of 2003 (the “FACT Act”). The rules were effective January 1, 2008, and all covered entities were required to comply no later than October 1, 2008.

The Affiliate Marketing Rules provide an additional degree of protection for consumers beyond the privacy requirements of the 1999 Gramm-Leach-Bliley Financial Services Modernization Act (“GLBA”), which requires financial institutions to allow consumers the right to opt out of information being shared with unaffiliated parties.

In summary, the new Affiliate Marketing Rules generally prohibit entities from using certain information received from an affiliate to make a solicitation to a consumer, unless the consumer is given notice and a reasonable opportunity to opt out of such solicitations.

“Affiliate” is defined as any company related by common ownership or common corporate control with another company. “Common ownership or common corporate control” is defined as ownership or control of 25% or more of outstanding shares of any class of voting security, control over a majority of directors, or power to exercise a controlling influence over management, as well any situation in which a person has one or more of these relationships with both companies.

Exceptions to the rules apply when:

- A company has a pre-existing relationship with the consumer (that is, if the specific business unit making the solicitation has a pre-existing relationship with a consumer, the rules don't apply, even if that unit received some information about the consumer from an affiliate), or
- A communication is initiated by a consumer, or
- The consumer requests or authorizes a solicitation.

If a consumer opts out of marketing, the election must be honored for at least five years from the date the opt-out is received. The new rules allow penalties of up to \$1,000 per violation, plus punitive damages and attorney's fees. Each solicitation (*i.e.*, each letter, telemarketing call, e-mail, etc.) would likely be considered a separate violation.

The new rules include model forms to facilitate compliance with the notice and opt-out requirement. Although use of the forms is not required, doing so provides a "safe harbor" for compliance with the FACT Act's requirement for clear, conspicuous and concise notices. The model forms also indicate the revisions and changes that may be made without losing the protection from liability they afford.

### Red Flag Rules

On October 31, 2007, the FTC and the federal financial regulatory agencies issued final rules (the "Red Flag Rules") requiring financial institutions and creditors to develop and institute written identity theft prevention programs, implementing Sections 114 and 315 of the FACT Act. The rules were effective January 1, 2008, and all covered entities must comply no later than November 1, 2008.

Under the Red Flag Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs (known as "red flags") of identity theft, such as unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime, and include a plan for updating the program. The program must be managed by the board of directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

The Red Flag Rules apply to financial institutions and creditors with covered accounts. "Financial institution" is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a transaction account belonging to a consumer. "Transaction account" is a deposit or other account from which the owner makes payments or transfers. "Creditor" is defined as any entity that regularly extends, renews, or continues credit, any entity that regularly arranges for the extension, renewal, or continuation of credit, or any assignee of an original creditor who is involved in the decision to extend, renew or continue credit. "Covered account" is an account used mostly for personal, family or household purposes, and that involves multiple payments or transactions.

The FTC and federal financial regulatory authorities issued guidelines, for use by financial institutions and creditors in developing their compliance programs, identifying five categories of red flags:

- Alerts, notifications or warnings from a consumer reporting agency;
- Suspicious documents
- Suspicious personally identifying information, such as a suspicious address
- Unusual use of – or suspicious activity relating to – a covered account
- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts

## Regulation R

This long-awaited joint regulation of the Federal Reserve Board and the Securities and Exchange Commission implements parts of the GLBA. That statute replaced the blanket exemption for banks from the broker-dealer registration requirements of the Securities Exchange Act of 1934 with a set of “activity-based” exemptions. For calendar year banks, it becomes effective January 1, 2009.

Some key provisions of Regulation R:

- GLBA permits “networking arrangements” in which banks and bank employees may refer customers to affiliated or unaffiliated “networked” securities brokers, subject to a number of requirements. Regulation R’s Rule 700 defines ways in which bank employees can be compensated for referrals, by defining what the statute means by a “nominal one time cash fee of a fixed dollar amount.” Rule 701 creates a non-statutory exemption that allows higher incentive compensation for referrals of institutional or high net worth customers.
- Securities transactions that are part of trust and fiduciary activities do not trigger a broker-dealer registration requirement if the bank engages in less than 500 securities transactions per year, or if the bank is “chiefly compensated” by “relationship compensation” as opposed to sales-based compensation. Rules 721 through 723 explain what these terms mean and how the “chiefly compensated” test can be met, on a bank-wide or account-by-account basis.
- Rules 740 and 741 define terms used in the statutory exemption for certain sweep transactions and create a broader exemption for certain sweeps into money market mutual funds.
- Rule 760 contains exemptions for banks that accept orders for securities transactions in custody accounts. Different rules apply for employee benefit plan accounts and IRAs, and for “accommodation” trades in other accounts.

These rules require attention from every bank that engages in securities transactions. The Federal Reserve Board recently published a summary of Regulation R focused on its impact on community banks. *The Small Entity Compliance Guide for Regulation R* may be found on the Fed’s Web site, [www.federalreserve.gov](http://www.federalreserve.gov).

## Regulation Z Amendments – Home Mortgage Loans

In July, the Federal Reserve Board adopted long-awaited amendments to Regulation Z, imposing a variety of requirements on all mortgage lenders (not just banks). All of the changes but those relating to escrow accounts become effective October 1, 2009.

For “higher priced mortgage loans,” there are a variety of new protections, including these:

- Lenders may not make a loan without regard to the borrower’s ability to repay. The rule proposal had prohibited only engaging in a “pattern or practice” of making such loans.
- Income and assets must be verified.
- No prepayment penalties may be charged for at least two years, and for the life of the loan if the payment can change in the first four years.
- Escrow accounts must be established for property taxes and insurance for all first mortgage loans.

The definition of “higher-priced mortgage loans” keys off an “average prime offer rate” to be published by the Federal Reserve Board, and is designed to capture subprime loans but exclude prime loans.

For all loans secured by a consumer’s principal dwelling – higher priced or not – other protections apply:

- Creditors and brokers cannot cause a real estate appraiser to misstate a home’s value.
- Mortgage loan servicers cannot engage in certain practices such as pyramiding late fees, must credit payments on the date of receipt and are required to furnish payoff statements in a reasonable time after receiving a request.
- “Good faith estimates” of loan costs must be furnished within three days of receiving any application for a loan secured by a principal dwelling – not just for home purchase loans.

Proposed requirements for charging “yield spread premiums” were withdrawn, although the Board said it would consider alternative approaches.

The Federal Reserve Board also has pending other changes to Regulation Z, as part of a package of proposals designed to prohibit unfair practices with respect to credit cards and overdraft services. These proposals, which have drawn a great deal of industry criticism, would also affect Regulation AA (Unfair or Deceptive Acts or Practices) and Regulation DD (Truth in Savings).

## Basel II Capital Rules

For the largest, internationally active U.S. banks that are required to adopt the new Basel II capital regime under final rules adopted in November 2007, the U.S. bank regulatory agencies continue to provide guidance. In July of this year, they published an Interagency Statement outlining how the extended qualification process will be conducted. Later in the month, the agencies published supervisory guidance on how the supervisory review process – the so-called “Pillar 2” of Basel II – will work. These large banks will be required to follow the “advanced approaches” under Basel II, unless they obtain a specific exemption.

Basel II also has a simpler “standardized” approach to calculating risk-based capital requirements. In June 2008, the agencies published a proposed framework for giving all other U.S. banks the option of using a U.S. version of the standardized approach. Under the proposal, U.S. banks would (with prior notice to the regulator) be able to elect to use this approach instead of the current rules, which are based on the old Basel Accord (“Basel I”). Generally, however, all affiliated banks in a holding company system would have to use the same approach, and a small bank holding company (under \$500 million in assets) could be exempt from applying the standardized approach to the parent.

As compared to current rules, the proposed Basel II standardized approach would expand the range of risk-weight categories to which credits may be assigned and use loan-to-value ratios to risk-weight most residential mortgage loans. Importantly, the proposed rules would add an explicit, separate capital charge for operational risk not included in the Basel I rules. This change would be calculated using the basic indicator approach under Basel II, which is based on a percentage of gross income.

The proposed rule would, like the advanced approach, also impose supervisory review requirements (Pillar 2) and new disclosure requirements (Pillar 3) designed to enlist market discipline on the capital-setting process.

These proposed rules replace an earlier notice of proposed rulemaking, issued in September 2006 and commonly called “Basel IA,” which was an attempt to tweak the current Basel I rules without moving to any of the Basel II approaches. The comment process persuaded the agencies that using the Basel II standardized approach created a better option for regulators and banks.

# Data Security: Federal Regulation

by Darren Baker  
Schiff Hardin LLP

Financial institutions certainly understand the need to keep customer data secure; it is simply a matter of good business, and what customers expect. But what particular steps are banks and other financial institutions required to take under federal law to protect customer information and what happens if a company does suffer a breach of such information? This article provides an overview of the most significant federal law applicable to financial institutions in the area of safeguarding sensitive customer information and related regulatory guidance, highlights some of the most prevalent failures in complying with these requirements, and provides tips to avoid making the same mistakes before a breach occurs or in response to one.

## The Gramm-Leach-Bliley Act

The primary federal law governing the protection of customer information is the 1999 Gramm-Leach-Bliley Financial Modernization Act (“GLBA”). GLBA applies to a broadly defined universe of financial institutions, including banks, securities firms and insurance companies, as well as companies that provide other financial services to consumers, such as tax preparation services, consumer loan services, credit reporting agencies, money transfer services, financial advisory services and debt collection. The GLBA’s provisions seek to protect from disclosure “nonpublic personal information” of customers, defined as personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless the information is otherwise publicly available. Among the provisions of GLBA is the so-called “Safeguards Rule.”

The Safeguards Rule requires all financial institutions to implement procedures to protect customer information from unauthorized use. A financial institution is required to implement security procedures that are appropriate to the institution’s size and complexity. The institution is given the power to determine the parameters of the program that should be in place, taking into account the type of activities it performs and the sensitivity of the customer information it collects. At a minimum, however, the rule requires that each company:

- Designate one or more employees to coordinate the information security program
- Identify and assess any reasonably foreseeable risks to the security and confidentiality of the customer information, and evaluate the systems currently in place to deal with such risks, including (i) employee training and management; (ii) information systems; and (iii) detection and prevention of, and responses to, any unauthorized access of data
- Design, implement and maintain a safeguards program consistent with the risk assessment performed, and regularly monitor and test that program
- Choose service providers that will maintain appropriate safeguards for the customer information and contractually require them to maintain appropriate safeguards and provide for monitoring and oversight of the service provider’s handling of customer information

- Evaluate and update the security procedures in light of relevant circumstances

## Compliance with GLBA

GLBA charges a number of federal agencies, including the Federal Reserve Board, Federal Deposit Insurance Corporation (“FDIC”), the Office of Thrift Supervision (“OTS”) and the Federal Trade Commission (“FTC”) with the implementation and enforcement of its provisions. The federal bank regulatory agencies tasked with enforcement of the GLBA provisions have issued guidance to provide clarity and assist financial institutions in safeguarding customer information and responding in the event of a security breach.

### *Guidelines for Establishing an Information Security Plan*

In 2001, the Federal Reserve Board, the FDIC, the OCC and the OTS issued *Interagency Guidelines Establishing Information Security Standards* (the “*Guidelines*”). In order to comply with the *Guidelines*, each financial institution must develop and maintain an information security program, the scale of which is appropriate for that institution. In developing and implementing the information security program, the *Guidelines* instruct financial institutions to undertake numerous actions, including engaging the board of directors or an appropriate committee of the board; undertaking an assessment of risk; and designing an information security program that includes training staff, regularly testing the key controls, systems and procedures, and developing, implementing and maintaining appropriate measures to properly dispose of customer information.

Each financial institution must also exercise appropriate due diligence in selecting its service providers, require its service providers by contract to implement appropriate security measures and monitor its service providers for compliance.

### *Guidance in Responding to a Breach of Sensitive Customer Information*

In order to assist financial institutions in responding to security breaches with respect to customer information, several agencies tasked to enforce GLBA’s Safeguards Rule also jointly released in 2005 the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (the “*Guidance*”). Under the *Guidance*, sensitive customer information includes a customer’s name, address or phone number, in conjunction with the customer’s social security number, driver’s license number, account number, credit or debit card number, or any personal identification number or password that would permit access to the customer’s account. Alternatively, any combination of components of customer information that would allow someone to log onto or access the customer’s account, such as user name and password or password and account number, also meets the definition of sensitive customer information.

The *Guidance* requires that every financial institution develop and keep in place a response program to address security breaches. At a minimum, the response program should call for the following actions in response to a security breach to comply with GLBA:

- The company must assess the nature and scope of the incident, and conduct a reasonable investigation to determine the likelihood that the information has been or will be misused.

- The company must identify which customer information systems and types of customer information have been accessed or misused in the breach.
- The company must notify its primary federal regulator of the breach as soon as possible.
- The company must notify appropriate law enforcement authorities consistent with Suspicious Activity Report (SAR) regulations.
- The company must take appropriate steps to contain and control the incident to prevent further unauthorized access to, or use of, customer information.
- If the company is mandated to notify its customers of the breach, it must do so in such a way that customers can reasonably be expected to receive it.

The *Guidance* also mandates that the customer notice should be given in a clear and conspicuous manner that includes a description of the incident and the types of information that were subject to unauthorized access. The notice must contain a listing of the measures taken by the institution to protect customers from further unauthorized access, a phone number that the customer may call for information and assistance, and a reminder to customers to remain vigilant over the next 12 to 24 months and to report suspected identity theft incidents to the institution.

If the financial institution determines the identities of the customers whose information has been breached, it may choose to notify only those customers whose information has been misused or where future misuse is reasonably possible. But if the institution cannot determine which customers' information has been breached amongst a larger group of files that might have been accessed, it must notify all members if misuse of their information is reasonably possible. E-mail notification is permissible if the company has been provided the customer's email address and the customer has agreed to receive email communications.

### Security Lapses and Enforcement Actions

In the years since passage of GLBA and the issuance of the *Guidelines* and *Guidance*, the agencies tasked with enforcement of GLBA have brought numerous actions against financial institutions challenging the data security practices with respect to sensitive consumer information and responses to breach of data security. In some cases, the agency charged that the company misrepresented the extent of its security measures, and in others that the data practices led to actual breaches and consumer injury. Agencies often issue a cease and desist order against a violator, followed by a civil monetary penalty and a consent order requiring corrective actions. The following are some of the key lapses in security that, in some cases, have spurred action by the agencies:

1. Failure to Maintain Secure Systems for the Storage of Data – Several companies have been the subject of enforcement actions because of their failure to sufficiently secure data and protect it from hackers. Practices that were highly scrutinized and criticized by regulators included the storage of data in unencrypted, clearly readable formats, storage of data for unnecessary lengths of time, failure to assess the vulnerability of systems to attack, failure to implement even simple, low-cost defenses to such attacks, and failure to employ measures to detect unauthorized access by hackers.

2. Unauthorized Release of Information – Several companies have drawn scrutiny for lax procedures in the sharing of customer information, leading to instances of identity theft or unintentional release of sensitive data to a large universe of people (such as the unintentional distribution of data in bulk e-mails). Practices such as failure to appropriately verify the identity of persons with whom data was shared, failure to effectively train employees to avoid unintentional disclosures and failure to maintain appropriate procedures to check for unauthorized disclosures have been criticized and noted in agency complaints and consent orders.

3. Failure to Secure Data from Rogue Employees or Comply with Privacy Policies – Many companies have been cited for failures to follow their posted privacy policies. In some cases, this has involved the sale of customer information in violation of the policy. In other cases, the company failed to secure data internally from unauthorized employees or from recently terminated employees with the incentive to utilize the information to draw negative publicity to the company. Still other companies have suffered from employees who failed to follow a recently amended privacy policy.

4. Stolen Hardware – There have been several instances in which confidentiality of customer information has been breached because of the theft of computer equipment such as laptops or backup tapes. In many cases, the threat was increased because data was not encrypted, and in other cases the security lapses have been exacerbated by failures of companies to comprehend the extent of the data theft, to quickly respond to the situation or to appropriately assess the risk arising from the theft.

In all of these cases, the financial institution that experiences a security breach will draw further ire of regulators and enhanced negative publicity if it does not have a plan for, and does not carry through with, appropriate notification of agencies and customers concerning the breach.

## Lessons Learned – Best Practice Tips in Complying with the Federal Data Security Requirements

While the consequences of exposed customer data are potentially serious, the good news is that with proper preparation and employee training, it is possible to minimize the chances of exposure. The following are a number of tips that will help keep your institution from becoming the next cautionary tale.

With respect to safeguarding customer information --

- Create an information security plan, but first implement low-cost measures quickly. Creating and implementing a comprehensive information security plan is required under GLBA and has always been part of the remedy required by consent orders. Not only does having an information security plan reduce the risk of security breaches, a plan helps prevent the agencies from arguing that the company was lax in its attempts to protect customers' personal information. However, if your company has no measures in place currently, do not delay. There are a number of simple security and technology measures that can be implemented quickly and at a reasonable cost. All companies should have anti-hacking software on computers that contain sensitive information, limit Internet access on these computers, and ensure that only

those employees who require access to these computers to perform their duties are able to log on.

- Create and follow a data retention schedule. When a company keeps customer data for longer than necessary it unnecessarily exposes that data to the possibility of access by hackers or other breaches of security.
- Keep close tabs on the location and safety of remote devices and other hardware. Not only should the company have a tracking system in place, it should also ensure that employees understand that a misplaced or stolen laptop can cost the company far more than the replacement cost of the device.
- Encrypt your company's stored sensitive data. In addition to decreasing the chances of a breach, most state breach notification laws exempt companies from notification requirements if the accessed data was encrypted. This fairly easy and inexpensive measure can save the company millions in legal fees, government fines and company time.

If, despite your best efforts, your customers' sensitive financial information has been exposed, it is still possible to minimize reputational and economic harm to your company by following a few simple guidelines

- When you are aware of the extent of the breach, inform the customers affected by that breach as quickly, fully and clearly as possible. Prepare a breach notification letter free of industry or legal jargon and release it as soon as the situation has been fully identified and isolated. (And be sure to take state law requirements into account – see our next article.) According to a survey, companies that notify customers of the breach via telephone or personalized letters, rather than email or form letters, are three times less likely to lose customers as a result of the breach.
- Immediately notify law enforcement and regulators of the breach. Doing so will increase the likelihood that they will view you as a partner rather than an obstacle in any subsequent investigation.
- Offer free credit monitoring to customers for the following year. This offer will increase the likelihood of maintaining your customers and help to minimize negative perceptions of the company.
- Treat all affected customers equally. When customers in several states are affected, it is best to disclose as much as required in the most stringent state to all customers regardless of their location. The unfavorable backlash the company will experience if customers become aware that others are receiving more disclosure than they are will almost certainly outweigh any benefit to be had by differing levels of disclosure.

# Data Security Breaches : State Law Consumer Notification Requirements

by Charlene Kalebic  
Schiff Hardin LLP

Virtually every company or organization maintains personal information on its constituents – including employees, customers, clients, patients, students and members. Financial institutions have a great deal of this type of information and some of it is required to be kept by law. Although some of it is still maintained the old-fashioned way in paper files, most of this personal information is maintained on the entity's computer information system.

Unfortunately, data security breaches of information systems are occurring more and more frequently – whether from a lost laptop, a diverted package shipment, or professional computer hackers – causing millions of individuals' personal information to be exposed to unauthorized persons, including identity thieves. The explosion of identity thefts caused by data security breaches has prompted the vast majority of state governments to enact legislation requiring those entities that are responsible for maintaining personal information to notify the affected individuals and, in certain states, governmental authorities and consumer credit reporting agencies in the event of a data security breach in which consumers' personal information is disclosed to unauthorized persons.

This is a fast-changing area of the law. As of September 30, 2008, over 40 states had enacted legislation requiring notification to consumers in the event of a data security breach, which is nearly double the number of states having consumer notification laws in 2006. While the laws vary widely from state to state, this article provides a general overview of the various state consumer notification laws with which entities are required to comply in the event of a data security breach.

## Who is Required to Notify?

Most state consumer notification laws are designed to protect the residents of the respective states. Therefore, a state's law generally applies to any business or organization that collects or maintains personal information on residents of that state, regardless of the location of the collecting or maintaining entity. Accordingly, if a company or organization has a national presence or if the data security breach has affected individuals of more than one state, the entity must comply with the respective state laws of the affected individuals, not simply the law of the state in which the entity is located.

## What Type of Information is Considered Personal Information?

Although the consumer notification laws vary slightly state by state, generally, for purposes of state consumer notification laws, information concerning a consumer is considered personal information if it contains unencrypted information with an individual's first name (or first initial) and last name in combination with any of the

following: (1) the individual's social security number; (2) the individual's driver's license number or state identification card number; or (3) the individual's account number or credit card or debit card number. Accordingly, the consumer notification laws do not apply in situations where a company's or organization's information has been disclosed, but rather only when an individual's personal information has been disclosed. However, for a number of reasons, one may wish to notify a company in the event the company's information has been disclosed due to a data security breach.

### What Triggers the Duty to Notify the Consumer?

When an entity has reason to believe that personal information that it maintains has been disclosed to unauthorized persons, it is required to notify the affected individuals. Even if the entity has taken all reasonable precautions to protect the personal information, and even if the disclosure was caused by criminal actions of others such as computer hackers, the entity maintaining the personal information has the duty to notify the affected consumer of the disclosure.

### When Should Notifications go to the Consumer?

State laws typically require notification in "the most expedient time possible without unreasonable delay" after the security breach has been discovered and after a reasonable time for an investigation into the matter to determine the scope of the breach and to restore the integrity of the information system. Although most states have not defined what is meant by "the most expedient time possible without unreasonable delay," at least one state has put an outside limit of 45 days from the date of discovery of the breach to provide notification. Most states also allow for a delay in notification if law enforcement officials determine that notification would impede a criminal investigation and provide the notifying entity with a written request to delay the notification.

### Who Must be Notified?

Any individual whose personal information has been disclosed who lives in any state with a consumer security breach notification law must be notified. While there are still a handful of states that have not passed consumer notification laws, it is advisable to notify affected individuals who live in these states as well.

In addition, approximately half of the states require notifying entities to notify the respective state attorney general, the state police, the applicable state agency responsible for cyber crimes or consumer affairs, the major consumer credit reporting agencies, or a combination of some or all of these groups.

### What Must be Included in the Notification?

The information required to be included in the notification varies widely from state to state. About half of the states that have enacted consumer notification laws have not specified any particular requirements that must be included in the notice, while the others list a number of details that must be included. For practical reasons, most entities will want to send the same notice to all affected individuals, regardless of their location. Accordingly, if an entity includes the following information in the notification, it will generally comply with the notification requirements of all the states except Massachusetts: (1) a description of the security breach and the approximate date of the breach; (2) the type of personal information that was disclosed in the breach; (3) contact information for the entity responsible for maintaining the information, including

the address and a telephone number of a contact person to call for additional information; (4) a description of the steps taken by the entity to protect the data from further security breach; (5) contact information for the major consumer credit reporting agencies; and (6) a reminder of the need to be vigilant for incidents of fraud and identity theft, and to report suspected incidents to law enforcement and the Federal Trade Commission.

Massachusetts, on the other hand, requires that the notice include information concerning: (1) the consumer's right to obtain a police report; (2) how the consumer can obtain a security freeze on their credit from the consumer credit reporting agencies and the information required when requesting a security freeze; and (3) any fees required by the consumer credit reporting agencies. Surprisingly, the notice in Massachusetts must not include the nature of the security breach or the number of Massachusetts residents affected by the breach.

### How Must the Notification be Made?

As a general rule, the notification must be made in writing. Notification may also be sent electronically if the notice is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §7001. In addition, many states allow for alternative forms of notice if the cost of notification is excessive (more than \$250,000 in most states), if there are a large number of affected persons who must be notified (more than 500,000 persons in most states), or if the entity does not have sufficient contact information on the affected individual. Under these circumstances, notification can typically be accomplished by electronic mail, posting to the entity's Web site, or notification to major statewide media.

### What is the Penalty for Failing to Timely Notify Consumers?

Penalties for failure to comply with the notification requirements vary widely by state. For example, Florida assesses a penalty of \$1,000 a day up to a maximum of \$500,000. Colorado, on the other hand, simply provides for the state attorney general to take "appropriate action" to ensure compliance with the law and to recover direct economic damages. Louisiana expressly provides for a civil action to recover actual damages resulting from the failure to notify.

In addition to the penalties imposed by the government, entities must also be mindful of civil lawsuits, including class action suits, that may be brought by affected individuals to recover damages as a result of the failure to provide timely notification.

### Conclusion

The Internet and computer information systems have forever changed the way that businesses and organizations conduct their affairs. It is hard to imagine any individual in modern society who has not provided his or her personal information to some business or organization, especially financial institutions. Security breaches will continue to plague entities that obtain and maintain personal information on individual consumers.

Until Congress passes a federal law with nationwide uniform consumer notification requirements in the event of a data security breach, financial institutions – like every other entity – must comply with the patchwork of ever-changing state consumer notification laws. Financial institutions that are in the unfortunate position of having

to provide consumers with notification of a data security breach should consult with legal counsel concerning the individual state requirements as soon as possible upon the discovery of a breach.

## Federal Officials Back Covered Bonds

by Lori Buerger  
Schiff Hardin LLP

On July 28, 2008, federal regulators joined with the Treasury Department in announcing support for residential covered bonds, with the stated goal of encouraging additional sources of mortgage financing and strengthening financial institutions. The Treasury Department issued a set of best practices designed to provide clarity to market participants. Earlier in July 2008, the Federal Deposit Insurance Corporation (“FDIC”) issued a *Final Statement of Policy* regarding covered bonds. On October 20, 2008, the Office of the Comptroller of the Currency (the “OCC”) provided additional guidance for national banks regarding covered bonds.

A covered bond market has long existed in Europe. With their actions, the Treasury Department and FDIC hope to encourage the use of covered bonds as a new class of mortgage-backed securities in the U.S. In a joint statement following the Treasury and FDIC announcements, JPMorgan Chase, Bank of America, Wells Fargo and Citigroup announced their support for the regulators’ efforts and plan to issue covered bonds.

### FDIC Statement

The FDIC’s *Final Covered Bond Policy Statement* became effective July 28, 2008, after a process that involved accepting comments approximately 130 parties. The statement outlines the availability of expedited access to collateral pledged for certain types of covered bonds, if the FDIC declines to continue the covered bonds after a bank failure. This is significant, because it allows access to the covered bond collateral after ten days, instead of the 45-90 days bond holders would generally be required to wait. In order to qualify for expedited access, covered bond issuances must be made with the consent of a financial institution’s primary federal regulator.

### Treasury Department Best Practices

The Treasury Department describes its Best Practices document as a “complement” to the FDIC policy. The Best Practices outline maturity periods, eligible collateral, required overcollateralization values, necessary disclosures, issuance limitations and monthly asset coverage tests for covered bond programs. Issuers must receive consent from their primary federal regulator before establishing covered bond programs, which will be granted only to well-capitalized institutions. The Best Practices state that covered bonds may be issued as registered securities or in transactions exempt from securities laws.

### OCC Guidance to National Banks

In Bulletin 2008-29, released October 20, 2008, the OCC provided guidance to national banks regarding satisfying the requirement for regulatory consent prior to the issuance of covered bonds. National banks must notify their examiner-in-charge and provide compliance information. The OCC will review the proposed programs under the supervisory no-objection process, and issue written supervisory no-objection to proposed covered bond programs.

## What is a Covered Bond?

The Treasury Department's Best Practices document provides a detailed definition of covered bonds. A covered bond is a secured debt instrument that provides funding to a depository institution, or issuer, that retains residential mortgage assets and related credit risk on its balance sheet. These assets are known as the cover pool. Interest on the covered bond is paid to investors from the issuer's cash flows, while the cover pool serves as secured collateral. Covered bonds provide dual recourse to both the cover pool and the issuer. In the event of an issuer default, covered bond investors first have recourse to the cover pool. In the event the cover pool returns less than par in a liquidation, investors maintain an unsecured claim against the issuer.

Covered bonds differ from mortgage backed securities in several ways. First, mortgages securing covered bonds remain on an issuer's balance sheet, unlike mortgage backed securities. Second, pools of loans securing covered bonds are dynamic, and non-performing or prepaying loans must be substituted out of the cover pool. Finally, if a covered bond accelerates and repays investors at an amount less than the principal and interest owed, investors retain an unsecured claim against the issuer.

Covered bonds differ from unsecured debt because the latter lacks secured collateral underlying the obligation of the issuer. While unsecured debt investors retain an unsecured claim against the issuer in the event of issuer default, covered bond investors possess dual recourse to both the underlying collateral of a covered bond and to the individual issuer. Accordingly, covered bonds provide investors with additional protection on their investment compared with unsecured debt. Generally, the advantages of covered bonds for issuers can include higher credit ratings, lower cost of funding and diversification of refinancing sources.

*Copies of the Treasury Department document are available at [www.treas.gov](http://www.treas.gov). Copies of the FDIC document are available at [www.fdic.gov](http://www.fdic.gov).*

## Schiff Hardin Financial Crisis Team

Schiff Hardin's Financial Crisis Team can provide comprehensive advice on the issues arising from the current financial and economic turmoil and the legislative and regulatory change it is producing. The Team helps clients evaluate and seize opportunities created by the Emergency Economic Stabilization Act and the Troubled Asset Relief Program. Lawyers from many of our practice groups also work together to help clients deal with increased regulatory oversight, criminal and regulatory investigations and civil litigation, as well as executive compensation, tax, real estate, bankruptcy, securities and labor and employment issues. Contact any member of the Financial Institutions Group listed on the cover of the *Financial Institutions Update*.



6600 Sears Tower  
Chicago, Illinois 60606

One Atlantic Center  
Suite 2300  
1201 West Peachtree Street  
**Atlanta**, GA 30309  
t 404.437.7000  
f 404.437.7100

225 Franklin Street  
Suite 2600  
**Boston**, MA 02110  
t 617.848.5750  
f 617.848.5784

6600 Sears Tower  
**Chicago**, IL 60606  
t 312.258.5500  
f 312.258.5600

One Westminster Place  
**Lake Forest**, IL 60045  
t 847.295.9200  
f 847.295.7810

900 Third Avenue  
**New York**, NY 10022  
t 212.753.5000  
f 212.753.5044

One Market  
Spear Street Tower  
32nd Floor  
**San Francisco**, CA 94105  
t 415.901.8700  
f 415.901.8701

1666 K Street, N.W.  
Suite 300  
**Washington**, DC 20006  
t 202.778.6400  
f 202.778.6460

1000 Skokie Blvd.  
Suite 215  
**Wilmette**, IL 60091  
t 847.920.9327  
f 847.920.9329

**Advertisement**

This publication is for the general information of clients and friends of our firm. It does not provide legal advice for any specific matter. Readers should consult a lawyer directly for such advice. This publication, or parts of it, may be considered attorney advertising material under professional conduct rules applicable to lawyers.