WILMER, CUTLER & PICKERING

ECOMMERCE NEWS

May 31, 2001

NEW DEVELOPMENTS: DATA SECURITY STANDARDS UNDER GRAMM-LEACH-BLILEY

Notices from financial institutions are filling consumers' mailboxes these days. But in addition to sending these notices, financial institutions have to ensure that they're complying with federal regulations concerning the secure treatment of data. What regulations? And what effect do these regulations have on contracts with vendors that process information for financial institutions? Here's a brief overview of the regulatory playing field.

Fast-approaching deadline. The compliance deadline under financial privacy regulations issued by various federal agencies under Title V of the Gramm-Leach-Bliley Act ("GLBA") is July 1. These regulations require "financial institutions" to provide certain individuals that obtain financial products and services from them with a notice describing how the institutions collect and disclose nonpublic personal information and the steps they take to safeguard that information and, in some cases, informing individuals of their right to opt out of certain types of information sharing.

Financial institutions have to guard the information they protect — but under what standards? Many companies that were startled to find themselves labeled "financial institutions" under the regulations' overbroad definition of the term are still scrambling to draft privacy notices and deliver those notices to their customers and/or consumers. In this mad rush toward compliance, many financial institutions have adopted or are adopting the language suggested by various agencies in the model notice provisions appended to each set of regulations. With regard to data security safeguards, for example, the model provisions suggest that financial institutions can meet the regulatory notice requirements by stating in part that they "maintain physical, electronic, and procedural safeguards ***that comply with federal regulations*** [or standards under some of the model clauses] to guard . . . nonpublic personal information."

As the dust settles on July 1, these institutions are faced with a question — just what are the applicable federal regulations or standards? For many institutions, there is no satisfactory answer.

Background. Title V of the GLBA requires certain federal agencies to create regulations not only addressing the privacy disclosure and opt-out obligations of financial institutions but also establishing data security standards. Specifically, the Act requires that the agencies "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards — (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." While all of the applicable agencies have released detailed and largely uniform financial privacy regulations, there has been no similar regulatory coordination with regard to data security rules. As a result, the data security requirements vary from agency to agency.

The Securities and Exchange Commission: The Parrot Approach

The SEC was the first to take any regulatory action with regard to the data security side of Title V of the GLBA. Rather than provide any concrete guidance as to the standards and safeguards applicable to financial institutions subject to its jurisdiction, however, the SEC parroted the GLBA's data security language in Regulation S-P — its financial privacy regulation. Under section 248.30 of the SEC's Regulation S-P, "[e]very broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information" and that are "reasonably designed to: (a) Insure the security and confidentiality of customer records and information; (b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer." As a result, entities subject to SEC regulation have no real guidance on what the applicable "federal standards" are with regard to data security.

The Banking "Interagency Guidelines" - General Directions Rather than a Roadmap

The banking agencies (the OCC, Federal Reserve System, FDIC, and OTS) went a step further than the SEC and issued data security "guidelines" (the "Interagency Guidelines") applicable to entities falling under their jurisdiction — largely traditional financial institutions such as banks, depository institutions, and bank holding companies. Although the Interagency Guidelines are directly applicable only to these traditional financial institutions, they could indirectly snare other companies such as service providers that assist banks in providing online services through outsourcing contracts, as discussed below.

The Interagency Guidelines do not contain mandatory procedures or measures to ensure compliance (such as encryption standards or requirements for the designation of a data security officer). Rather, the agencies chose to preserve a flexible approach that allows each institution to determine the best way for it to protect data security given its size and complexity and the nature and scope of its activities. Although the Guidelines do not require the adoption of specific data security measures, they do require institutions to create a data security program tailored to the institution's needs, and they specify steps that institutions must follow in crafting that program, including the active involvement of the board of directors or a committee of the board in overseeing the development of the program, approving the program, and overseeing its implementation and maintenance.

Scope of the Interagency Guidelines. The Interagency Guidelines require an institution to adopt a comprehensive written security program that includes administrative, technical, and physical safeguards designed to meet the three objectives listed in the GLBA — (1) to ensure the security and confidentiality of customer information, (2) to protect against anticipated threats or hazards to the security or integrity of customer information, and (3) to protect against unauthorized access to customer information that could result in substantial harm or inconvenience to any customer. The Guidelines specify that the program need only apply to "customer information," defined as "any record containing nonpublic personal information . . . about a customer [as those terms are defined in the financial privacy regulations], whether in paper, electronic, or other form, that is maintained by or on behalf of the bank."

Because the Guidelines incorporate the definition of "customer" from the financial privacy regulations, the institution's information security program does not need to protect information about individuals who do not have a *continuing* relationship with the financial institution ("nonconsumers" or "consumers"), individuals who obtain financial products or services for business, agricultural or commercial purposes, or business entities. The definition of "customer information" covers full records — *e.g.*, complete files -- that contain any nonpublic personal information, even if the records contain only a small amount of such information, although the amount of nonpublic personal information contained in a record would be a relevant factor in deciding what level of protection to afford to that record.

Steps to Creating an Information Security Program. Under the Interagency Guidelines, an institution must first conduct a risk analysis to identify reasonably foreseeable internal and external threats that could result in the unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. ("Customer information systems" are defined broadly as "any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.") The analysis must assess the likelihood and potential damage of threats and the sufficiency of current risk controls used by the institution. Once the risk assessment is complete, the institution must design a written information security program to control the identified risks.

In designing the program, the institution is directed to *consider* (although not necessarily to adopt) specific listed measures to control risk, such as access controls or restrictions, encryption, monitoring systems, dual control procedures, and employee background checks. Additionally, the institution is required to train its staff to implement the final information security program as well as to regularly test the key controls, systems and procedures upon implementation of the program.

Vendor Contracts. In addition to implementing an internal information security program, the Interagency Guidelines require a financial institution to take certain steps to ensure that its service providers maintain appropriate data security safeguards. When using a service provider, the financial institution must: (1) exercise appropriate due diligence in selecting service providers; (2) contractually require service providers to implement appropriate data security measures; and (3) where indicated by the institution's risk assessment, monitor its service providers to confirm that they have satisfied their data security obligations. Although a financial institution must contractually require its service provider to implement "appropriate" data security measures, those measures need only be designed to meet the data security objectives and need not be identical to the measures set forth in the financial institution's data security program nor must they comply in other respects with the Interagency Guidelines. ***Contracts entered into on or after March 6, 2001 must include such data security provisions effective July 1, 2001; contracts entered into on or before March 5, 2001 must be amended to include appropriate data security provisions by July 1, 2003.***

Under the Guidelines, a "service provider" is defined extremely broadly as "any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank." The definition does not include, however, any subservicers that a service provider may hire; in other words, a financial institution is *not* responsible for overseeing subservicers nor must it require subservicers to have in place appropriate data security measures. However, as part of its due diligence in selecting the original service provider, it must determine whether that provider has adequate controls to ensure that a subservicer will protect customer information in a way that meets the objectives of the Guidelines.

Adjustment and Monitoring of the Information Security Program. After a financial institution implements its information security program, its obligations under the Guidelines are not terminated. Rather, the financial institution must monitor and adjust the program in light of any relevant changes, including updates in technology, changes in the sensitivity of the customer information it gathers, differences in internal or external security threats, and changes in its business structure or arrangements. As part of this monitoring, it must report to its board of directors or an appropriate committee of the board at least annually on the state of its information security program and its compliance with the Guidelines.

The Federal Trade Commission's "Safeguards" Rule - Not Even Out of the Starting Gate

In contrast, the FTC, which has jurisdiction over most of the "nontraditional" financial institutions such as internet companies that engage in "screen scraping" or other financial data processing or transmission services, has stalled in its efforts to create a data security rule. Despite issuing an Advanced Notice of Proposed Rulemaking last September, the FTC has yet to release a Notice of Proposed Rulemaking. Best

estimates suggest that an NPRM may be released some time this summer. Factoring in the comment period and the time needed for the agency to draft a final rule, it would seem unlikely that a final rule will be released before next fall at the earliest.

Nor does the Advanced Notice of Proposed Rulemaking provide any real insight on where the FTC might be headed in drafting a proposed rule. Rather, the notice consisted of an information gathering tool soliciting industry perspectives on a variety of issues relating to data security and throwing out many alternative approaches that could be taken in crafting a final rule. Despite the uncertainty, there is some evidence that the FTC might create more specific minimum standards as opposed to the open, flexible approach in the Interagency Guidelines.

For example, the FTC requested comment on whether it should provide more detailed and specific guidance than that provided by the Interagency Guidelines and whether it should issue binding rules as opposed to guidelines. Noting that, unlike the FTC, the banking agencies conduct periodic reviews such as safety and soundness reviews of entities within their jurisdiction, the FTC hypothesized that more concrete standards may be required for entities subject to its jurisdiction. However, only time will tell which approach the FTC will take.

What's a financial institution to do?

In the absence of true federal "standards" or "regulations" as to appropriate data security measures, what must a financial institution do to satisfy the likely representation in its privacy notice that its physical, electronic, and procedural data security safeguards comply with federal regulations or standards?

The Interagency Guidelines, although inapplicable to entities outside those agencies' jurisdiction, could be used as a general template for the process of creating a compliant data security program, but that still leaves the open question of what elements are required in that program. The likely best answer for the moment is to look to industry standard practices. If the industry standard for data security on electronic systems, for example, requires use of PIN numbers or encryption, then a company following that standard has a strong argument that, despite the absence of true federal guidance, its data security program complies with applicable standards.

On the other hand, if a company fails to keep pace with industry standards, it will likely have an uphill battle in the event an agency or consumer group challenges its data security measures — especially if lax measures result in security breaches leading to data corruption or leakage.

Several organizations have issued their own guidance regarding appropriate security safeguards that can be used as resources in determining what data security risks exist and what safeguards to implement:

- The Department of Energy Computer Incident Advisory Center (www.ciac.org);
- WebTrust (www.aicpa.org/webtrust/princrit.htm), a security assurance service offered by AICPA and VeriSign; and
- CERT/CA (www.cert.org), a reporting center for internet security problems that is affiliated with Carnegie Mellon University.

For more information about complying with data security standards under the GLBA, contact:

Becky Burr	bburr@wilmer.com	202/663-6695
Susan Crawford	scrawford@wilmer.com	202/663-6479
Ron Greene	rgreene@wilmer.com	202/663-6285
Satish Kini	skini@wilmer.com	202/663-6482
Scott Llewellyn	sllewellyn@wilmer.com	202/663-6171
Tacha Steimer	nsteimer@wilmer.com	202/663-6534

ECommerce News is a publication of WCP's EGroup.