



The CLOCK Is Ticking On PRIVACY

By Paul Dillard, Senior Examiner, Federal Reserve Bank of San Francisco

With the recent passage of the Gramm-Leach-Bliley Act (GLBA), financial institutions can look forward to some rather complicated gymnastics to address the issues of customer privacy under the new Privacy of Consumer Financial Information (Regulation P), and the information systems integrity portion of the statute.

Per the consumer disclosure requirements referenced in GLBA and enforced by Regulation P, financial institutions will have to provide non-business customers with:

- An initial notice describing the institution's privacy policy;
- An annual notice reiterating the privacy policy thereafter for the life of the account relationship; and
- An opportunity to "opt out" of having their nonpublic personal information shared.

Regulation P becomes effective November 13, 2000; however, mandatory compliance has been deferred until July 1, 2001. This reprieve acknowledges the time and resources required to implement the necessary information system changes to ensure full compliance, particularly for small financial institutions, which are not exempted.

Before a financial institution charges ahead, the following significant questions need to be asked:

- Does the institution currently have a privacy policy in place?
- If so, does the institution actually follow its policy? (This may sound like a silly question. But, a recent informal survey conducted by a leading industry consultant yielded the surprising statistic that no more

than 50 percent of financial institutions that currently have privacy policies even follow them.)

- Does the institution want to share customer information beyond its affiliated companies?
- If so, has the institution developed the required opt out notices?

Another component of GLBA concerns the integrity of an institution's information systems. While there is no forthcoming regulation on the subject, interagency guidelines for meeting the information systems requirements with respect to customer records have been issued for comment. These guidelines require financial institutions to take appropriate action to:

- Ensure customer record security and confidentiality;
- Protect the security and integrity of customer data and information systems; and
- Protect against unauthorized access.

In addition, some financial institutions may face the specter of state initiated legislation which, if more restrictive, may preempt federal law. In response to those public advocates who feel that GLBA falls short of providing sufficient consumer privacy in such a dynamic electronic banking environment, many states have introduced their own customer privacy legislation.

As of April 21, 2000 more than 100 bills had been introduced by 41 states. The focus of this legislation has been to regulate the use of information collected online by service providers and web sites, and to ban or limit financial industry use of account related infor-

mation. Another popular theme among state legislation has been an "opt in" approach as opposed to GLBA's "opt out." This creates serious programming resource implications for financial institutions operating across state lines and in an environment with different state Privacy requirements.

At a recent trade industry gathering, attendees provided a broad perspective on Privacy and made some insightful observations:

- Larger financial institutions are approaching Privacy from an "enterprise wide perspective." They are designating senior officers to oversee their Privacy efforts. Moreover, these efforts are not performed in a vacuum, but rather they are coordinated throughout the institution;
- Many stated they are starting Privacy preparations early rather than waiting until the last calendar quarter prior to mandatory compliance. This more prudent approach reflects the complexity and far reaching consequences of their task;
- Also, in an effort to minimize the potential for more restrictive state legislation, financial institutions are leaning toward self-policing. For example, some are expanding the definition of protected information beyond that stipulated in Regulation P to include a customer's medical information or credit and debit card purchases.

Whatever their final business decisions may be, financial institutions are recognizing the soundness of addressing Privacy concerns before time runs out!

CI