Financial Privacy and Identity Protection Regulations

Privacy of Consumer Financial Information
Regulation P, Privacy of Consumer Financial Information, implements the GLBA financial privacy provisions. Through the GLBA, Congress restricted the ability of banks to disclose customer information to third parties. The law and regulation also require banks to provide customers with a notice of their privacy policy when a banking relationship is established and annually thereafter. Customers can opt out of certain disclosures of personal financial information.

To protect customer information and other bank data, federal regulators and sound business practices require banks to be prepared to respond to any security breach. Recognizing that every bank is susceptible to improperly configured systems and to software vulnerabilities, regulators have adopted rules requiring financial institutions to put in place incident response programs (IRPs) that follow certain standard procedures. Moreover, laws in most states mandate that individuals be notified if there is a breach in the security of electronically held customer information.

Interagency Guidelines on Information Security
Banks regularly collect personal information from their customers, such as their names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. Section 501 of the GLBA requires financial institutions to ensure “the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer.”

To assist banks in implementing the requirements of Section 501, bank regulators issued the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, commonly known as the Safeguards Rule. The Safeguards Rule requires banks to have a comprehensive written information security program that:

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

In addition, banks must have standards for the proper disposal of customer information, which is also a requirement of the Fair and Accurate Credit Transactions Act (FACT Act).

Interagency Guidance on Internet Authentication
In 2001, federal banking regulators issued guidance on methods for verifying the identity of customers using electronic banking services. Titled “Authentication in an Internet Banking Environment,” the guidance provides direction for evaluating and implementing authentication systems and practices. Although the guidance, updated in 2005 and again in 2011, focuses on Internet banking delivery channels, it also applies to all types of electronic banking. The guidance’s purposes are to safeguard customer information, prevent money laundering and terrorist financing, reduce fraud, inhibit identity theft, and promote the enforceability of electronic agreements and transactions.

Protecting Children Online
In 1998, Congress enacted the Children’s Online Privacy Protection Act to prohibit unfair or deceptive acts or practices in the collection, use, or disclosure of personal information from and about children on the Internet. The act protects the privacy of children and requires operators of websites directed toward children to obtain consent from parents before collecting data about their children.
Financial Privacy and Identity Protection Regulations

Right to Financial Privacy
One of the older privacy laws, the Right to Financial Privacy Act, was passed in 1978 to protect the financial records of individuals from unwarranted access by the federal government. The act establishes criteria under which federal government agencies may obtain financial records and imposes a duty on financial institutions to screen requests for information to ensure they meet the requirements of the law before releasing the requested records.

State Requirements Protecting Social Security Numbers
Most states have laws restricting the use or dissemination of Social Security numbers (SSNs). These restrictions are often included in state information privacy and security laws. Because bankers handle SSNs for a variety of purposes, it is important for them to know the requirements of their respective state laws. In general, these state laws prohibit:

- Publicly displaying, intentionally communicating, or otherwise making an SSN available to the general public
- Intentionally printing an SSN on a card required to access goods or services or to enter a location (such as an employee identification card)
- Requiring a customer to transmit an SSN over the Internet unless the connection is secure or the SSN is encrypted
- Requiring a customer to use an SSN to access a website unless a password, a unique PIN, or other authentication is also required
- Printing an SSN on any materials that are mailed to a customer unless required by law

Most state laws do, however, have exceptions for using SSNs for internal verification needs, fraud investigations, or administrative purposes associated with legitimate banking functions.

Red Flags Rule
One of the requirements of the FACT Act directs banks to develop and implement written identity theft prevention programs. Bank identity theft prevention programs must include policies and procedures for identifying and detecting warning signs—or “red flags”—of identity theft. These requirements are more commonly known as the Red Flags Rule. An identity theft program must also spell out appropriate actions the bank will take when red flags are detected, and it must be periodically updated to reflect new risks.