



# Gramm-Leach-Bliley, Title V and Reg. P

Complying with the  
federal privacy statute and its  
implementing regulations

Fred Everett  
Senior Vice President  
Countrywide Home Loans, Inc.

# Background

- Passed in 1999 as part of a broader bill to “modernize” financial services
- Applies only to “financial institutions”
- Provides a “floor” for consumer protections – no preemption
- Administrative enforcement only – no private right of action
- Federal Functional Regulators (OTS, OCC, etc.) plus the FTC.

# Overview

- Describes *when* information may be shared between nonaffiliated entities
- Describes *how* the information must be protected
- Describes *what* financial institutions must do if information is shared with unauthorized third parties

# Sharing Information

- Definition of “non public personally identifiable information” (NPPI):

“means any information a consumer provides to a bank to obtain a financial product or service...[any information] about a consumer resulting from any transaction involving a financial product or service between a bank and a consumer...or [any information] the bank otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.” – Reg. P, Sections 216.3(n) and (o).

As a starting point for analysis, any information that is not in a public forum should be considered NPPI.

# How can we share NPPI?

Prior to sharing NPPI with an unaffiliated third party, a financial institution must:

- ✓ Provide the customer or consumer with a notice that describes its policies and practices with regard to sharing.
- ✓ Wait a “reasonable time” to allow the consumer or customer to exercise their right to “opt out” of any sharing.
- ✓ Annually provide customers with a copy of its privacy notice and opportunity to opt out.

# Sharing NPPI

- If customers “opt out”, financial institutions must NOT share the customer’s NPPI with third parties.
- There are exceptions to this general prohibition on sharing after an “opt out”.
- Affiliate information sharing is generally covered by another law –The Fair Credit Reporting Act (FCRA).

# Protecting NPPI

- The “Safeguards Rule” or the “Interagency Guidelines Establishing Information Security Standards”.
- Implements Section 501(b) of GLBA
- Final Rule effective May 23, 2003
- Provides standards for financial institutions to follow to insure the security of NPPI, regardless of whether it is shared.

# Protecting NPPI Under Reg. P

- The Interagency Guidelines mandate:
  - All financial institutions must have an “Information Security Program” (ISP) that is designed to achieve the “objectives”:
    - Insure the security and confidentiality of customer information
    - Protect against any anticipated threats or hazards to the security or integrity of such information, and
    - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
  - The ISP must be comprehensive and contain administrative, technical and physical safeguards.
  - Financial institutions have flexibility in designing their ISP depending on their size, complexity, nature and scope of activities, and the sensitivity of the customer information at issue.

# Required Elements of an ISP

- Designated employee to head up
- Employee training
- Information systems involvement
- Detection, prevention and response to attacks and intrusions
- Implementation of safeguards to control identified risks and regular tests of same
- Adjust program on a go-forward basis
- Require service providers to protect NPPI

# Breach Notifications

- Additional set of regulations from the federal regulatory agencies under their Section 501(b) authority
- Supplements the “Safeguards Rule”
- Required policy should be included with the Information Security Program

# Response Program Components

- Assess the nature and scope of any incident, including affected systems and types of customer information affected
  - Notify primary federal regulator as soon as possible in cases where “sensitive information” has been breached
  - Notify law enforcement where appropriate
  - Take steps to contain and control the incident and prevent further breach
- **Notify Customers:**
    - When sensitive information is breached and
    - When the financial institution determines that misuse has occurred or is likely to occur
    - Notice to be sent “as soon as possible” consistent with the legitimate needs of law enforcement to delay notice

# “Sensitive Information”

“...means 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 a personal identification number or password that would permit access to the customer’s account. ...[A]lso includes any combination of components of customer information that would allow someone to log into or access the customer’s account, such as a user name and password or password and account number.”

# Customer Notice Content

- **Must Include:**
  - Clear and conspicuous language
  - Describe the incident in general terms and the type of customer information that was breached
  - Describe what the financial institution has done to protect from further breach
  - Telephone number to call for additional information
  - Remind customers to remain vigilant for the next 12-24 months
- **Should include, if appropriate:**
  - Recommendation to review statements and report suspicious activity
  - Description of fraud alerts and how one can be placed
  - Recommendation to periodically obtain credit reports to detect fraudulent transactions
  - An explanation of how to obtain free credit reports
  - Information on FTC website and availability of assistance and encouragement to report incidents to FTC.

# State Laws on Breach Notice

- Many States have passed laws requiring notice of security breach to affected customers.
- These laws vary in terms of definitions of the types of data that, when breached, require consumer notification
- Some require specific involvement and notification of law enforcement agencies.