

# Customer Information Security and Privacy Requirements under Gramm-Leach-Bliley

# DRG Disclaimer

- ❖ *Not Legal or Privacy Experts – we do not interpret Privacy Legislation*
- ❖ We are Security Experts
- ❖ We focus on the Financial Services sector
- ❖ Knowledgeable and experienced on the newest and latest technologies for Information Protection
- ❖ Here today to provide a short overview on Gramm-Leach-Bliley Act.

# Recent Security Legislation

- ❖ **Gramm-Leach-Bliley (GLB) Act**
- ❖ VISA Cardholder Information Security Policy (CISP)
- ❖ E-Sign Act
- ❖ Health Insurance Portability Accountability Act (HIPAA)

# GLB Act - Overview

- ❖ Companies Covered by GLB Act:
  - ❖ Generally, any enterprise “engaging in financial activities...”
- ❖ Effective Date: July 1, 2001 and thereafter
  - ❖ Experts expect some lag before enforcement and fines are imposed
  - ❖ Changes in technology and in partners/vendors will require ongoing security reviews and testing
- ❖ Penalties:
  - ❖ Extensive fines
  - ❖ Up to 10 years imprisonment

# GLB Act - General

- ❖ Requires Financial Services Providers (FSPs) to secure customer's personal information against any "reasonable foreseeable" internal or external information threats to their security, confidentiality, and integrity
- ❖ Establishes FSP "affirmative & continuing obligation"

# GLB Act - Applicability

## Applicability:

- ❖ Applies to those “engaging in financial activities as described in Sec 4(k) of the Bank Holding Company Act” of 1956.
- ❖ Includes, but is not limited to:
  - Appraisers
  - Data Processors
  - Insurance Agencies
  - Tax Preparers
  - Collection Agencies
  - Finance Companies
  - Retailers issuing their own credit cards
  - Financial Advisors
  - Check Cashing Services
  - Leasing Agencies
  - Travel Agencies
  - Investment Advisors

# GLB Act - Responsibility

- ❖ FSP's Board of Directors – have ultimate responsibility for compliance
- ❖ BOD must be actively involved with developing, writing, approving and implementing – normal oversight
- ❖ Management may be delegated supervision of operations
- ❖ Board must receive report annually



# GLB - Privacy

## Regulation P

- Governs allowable uses of personal consumer information
- Limits sharing of consumer info with unaffiliated third parties
- Makes privacy policies known to consumers prior to purchases
- Makes reasonable efforts to ensure privacy disclosures are clear and conspicuously identified / received – annually
- Provide easy method for “opt out” completely or partially of third party info sharing at any time
- Consumer info may be shared with FSP’s service providers without consent
- However, FSP procedures and levels of confidentiality must be maintained.

# GLB - Security

REQUIRES: develop customer information security programs to:

- ❖ Ensure the security and confidentiality of customer information
- ❖ Protect against any anticipated threats to the security or integrity of customer information
- ❖ Safeguard against any unauthorized access or use of customer information resulting in customer inconvenience or harm

# GLB - Info Sec Requirements

Requires organizations to address five key InfoSec areas:

1. Assess IT environments and understand security risks
  - Formally define both internal and external risks
2. Scrutinize business relationships for adequate security
  - Need to ask partners about their security programs, security practices, and ensure they are aligned with your risk tolerance and own security practices
3. Provide user training and security awareness programs
  - Ensure employees are properly trained in security procedures and policies

# GLB - Info Sec Requirements

Five Key InfoSec areas (continued):

4. Establish information security policies
  - Install controls for internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer info and customer info systems
  - Encouraged to implement system detection and record attempted attacks
5. Perform independent assessments
  - Sufficient testing based on frequency of change in technology, threats, and systems

# GLB - Info Sec Requirements

Customer information security programs must:

- ❖ Be reviewed and updated annually
- ❖ Tested periodically and adjusted, as necessary (technology, data classification, internal/external threats)
- ❖ Level of protection may vary with data sensitivity for each category

# DRG Background

- ❖ *Leading Internet Security Company*
- ❖ Securing Business since 1997
- ❖ Focus: Security Solutions and Services
- ❖ Industry Focus: Financial Services
- ❖ Headquartered in Redwood Shores, CA
- ❖ Independent Security expertise

# Financial Customers

❖ Wells Fargo Bank

❖ Citigroup

❖ Charles Schwab

❖ Providian Financial

❖ Bank of Montreal

❖ First Data

❖ 724 Solutions

❖ iPIN

# DRG Security Services

## Financial Industry Solutions Team

- ❖ Perform Security and Risk Assessment
  - ❖ Internal security programs/applications
  - ❖ Review Existing third-party partners
  - ❖ Due diligence for potential partners
- ❖ Develop Security Policy and Programs
- ❖ Evaluate Internal and External Threats
- ❖ Provide Security Awareness Training

# DRG Security Consulting

Digital Resources Group LLC  
270 Redwood Shores Pkwy #210  
Redwood Shores, CA 94065  
650-508-8959  
Info@drgsf.com

**[www.drgsf.com](http://www.drgsf.com)**