



should be considered NPPI

**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.

**Protecting NPPI Under Reg. P**

**Required Elements of an ISP**

**Response Program Components**

**“Sensitive Information”**

**Customer Notice Content**

**Paul H. Schieber**

Title: Chairman of Blank Rome LLP's  
Consumer Financial Services/Retail

**Privacy: Gramm-Leach-Bliley Act Overview**

<b><u>Financial Privacy Rule</u></b>
<b><u>Consumers and Customers</u></b>
<b><u>Types of Notices:</u></b>
<b><u>Delivery of Privacy Notice</u></b>
<b><u>Opt-Out Rights</u></b>
<b><u>Who Must Comply and How to Comply</u></b>

**How to Comply**

- Designate one or more employees to coordinate the safeguards;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select appropriate service providers and contract with them to implement safeguards; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of

safeguards.

**Employee Management and Training**

- Check references prior to hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.
- Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
  - locking rooms and file cabinets where paper records are kept;
  - using password-activated screensavers;
  - rapid screen lock-outs;
  - using strong passwords (e.g., eight characters long);
  - restricting cell phone cameras;
  - restricting iPods;
  - Instruct and regularly remind all employees of your organization's policy - and the legal requirement - to keep customer information secure and confidential.
  - Provide employees with a detailed description of the kind of customer information you (they) handle (name, address, account number, and any other relevant information) and post reminders about their responsibility for security in areas where such information is stored.
  - Limit access to customer information to employees who have a business reason for seeing it.
  - Impose disciplinary measures for breaches.
- Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Suggestions on how to maintain security data entry to data disposal:
  - Store records in a secure area. Make sure only authorized employees have access to the area. For example:
  - store paper records in a room, cabinet, or other container that is locked when unattended;
  - ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;

**Employee Management and Training**

**Information Systems**

**Records Destruction**

**Paper:**

**Electronic Media:**

**Managing System Failures**

**Vendor Contracts**

**Cross Border Connections**

- store electronic customer information on a secure server that is accessible only with a password - or has other security protections - and is kept in a physically-secure area;
- don't store sensitive customer data on a machine with an Internet connection;
- maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area; and
- use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.

**Practical Contracting Tips:**

- Define "security breach"
- Vendor must notify data owner/licensee of breaches; must do so timely and with all details
- Vendor to cooperate with and assist data owner/licensee and law enforcement; to include assisting owner/licensee with breach notices, obtaining owner/licensee approval for all vendor notices
- Automatic amendment of vendor obligations to comply with changes to applicable law

**Name: John L. Jones**

Title: President of Arionzoe - Corp.

**Information Security Model, Process and Outputs**

*In some cases, consequence severity may not change. The goal then is to drive "likelihood of occurrence" to zero.*

<b><u>Security Breaches</u></b>
<b><u>Varying state notification requirements</u></b>
<b>Practical Contracting Tips:</b>
<b>Information Security Method</b>
<b>Managing Information Risk</b>

Security Solutions: Model/Process/Outputs	
Information Security Model	
<b>Solution:</b>	
<b>Support Program:</b>	
<b>Awareness Program:</b>	
Information Security Process	

**Information Security Model:**

1. Business & Risk Description (Foundation)
2. Policy and Architecture (Framework)
3. Solution Specification (People, Processes & Technology)
4. Support (Testing, Maintenance & Sustainability)
5. Education (Initial and Continual)

*“Assess and Re-assess Risk Throughout Process”*





