FOLEY EXECUTIVE BRIEFING SERIES

Securing Data in Technology Transactions

Matthew Karlyn, Senior Counsel
Peter McLaughlin, Senior Counsel

FOLEY
FOLEY & LARDNER LLP

©2010 Foley & Lardner LLP • Attorney Advertising • Prior results do not guarantee a similar outcome • Models used are not clients but may be representative of clients • 321 N. Clark Street, Suite 2800, Chicago, IL 60654 • 312.832.4500

Agenda

- Overview of the data security/compliance landscape
- Understanding where your risk is
- Tips for drafting and negotiating data security provisions
- Practical examples of provisions
- Top 10 recap

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Why is information security so important & visible?

- Increased federal regulations Sarbanes Oxley, HIPAA, GLBA and FTC regulations
- Increase in state legislation for security breach notification
- Industry regulations such as PCI.
- Increased access by third parties to organizations' most valuable information assets.
- Increased dependency on technology to operate every aspect of business
- Increased use of business processes like web portals that provide customer self-service.
- Reasons of national security
- The identity theft and fraud boom
- The increase in number of security incidents

©2010 Foley & Lardner LLP

What information security standards exist?

- Global
  - ISO 17799, 27001
  - Basel II, EU Safe Harbors
  - Country Standards
- National – NIST & OECD
- Finance – CoBIT & BITS
- Federal Government
  - DOD · Rainbow Series, NIST
  - NSA
- Presidential Directives
- State Laws – MA 201 CMR 17.00 & other state data security and breach notification laws
- Industry
  - Payment Card Industry Data Security Standard
  - Healthcare – HIPAA
  - Finance – Gramm Leach Bliley, SEC, NASD, FFIEC, OTS
  - Energy and Utility – NERC 1300, FERC, (NEI 04-04)
  - E-Commerce – FTC E-commerce Req's

©2010 Foley & Lardner LLP

Massachusetts regulations (201 CMR 17.00)

The Regulations impose two main requirements:

(i) the duty to develop, implement and maintain a very comprehensive written information security program that meets very specific requirements; and

(ii) the obligation to meet specific computer information security requirements

©2010 Foley & Lardner LLP

FTC Legal Authority

- Section 5 of the Federal Trade Commission Act ("Section 5") prohibits "unfair or deceptive acts or practices in or affecting commerce."
  - **Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information.**
  - **Also requires companies holding sensitive data to have in place reasonable procedures to secure it if the failure to do so is likely to cause substantial consumer injury.**

©2010 Foley & Lardner LLP

FTC Reasonableness Standard

- Process-oriented approach that emphasizes **identifying and mitigating risks**
- There is **no one size fits all solution** – take into account the size and complexity of the business operations and the sensitivity of the information at stake

©2010 Foley & Lardner LLP

Regulatory Language Should be Treated as a Floor

- Including the HIPAA, GLB, and other statutory/regulatory minimally-required security language, without more, does not adequately protect companies.
- Even the more robust language provided in laws and regulations (e.g., HIPAA Security Rule, GLB Safeguards Rule, etc.) do not provide sufficient protection.

©2010 Foley & Lardner LLP

General Info-Sec Risks (“CIA”)

- Confidentiality: **ensuring that data is accessible only to those authorized to have access**
- Integrity: **safeguarding the accuracy and completeness of data**
- Availability: **ensuring that authorized users have access to data when required**

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Understanding Risk

- Understand what data is in question
- Where do you want/need the data to flow
- Compliance decisions and resources
- Policies and procedures
- Awareness and enforcement

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

General Control Types

- Administrative Controls – **"include the development and publication of policies, standards, procedures, and guidelines, the screening of personnel, security awareness training, the monitoring of system activity, and change control procedures."**
- Technical Controls: **"consist of logical access control mechanisms, passwords and resource management, identification and authentication methods, security devices, and configuration of the network."**
- Physical Controls: **"entail controlling individual access into the facility and different departments, locking systems and removing unnecessary equipment, protecting the perimeter of the facility, monitoring for intrusion, and environmental controls."**

Sources: Shon Harris' excellent "CISSP Certification Exam Guide" and Tipton and Krause book titled Information Security Management Handbook,

©2010 Foley & Lardner LLP

Information Security Contracting

©2010 Foley & Lardner LLP

The Problem

- Companies have developed sophisticated approaches to information security within their own organizations, but fail to adequately address the more general issue of information security in their vendor and business partner relationships.

©2010 Foley & Lardner LLP

1. Vendor Due Diligence

- Common Errors
  - Failure to involve all relevant stakeholders in the process
  - Failure to assess the unique requirements of the transaction
  - Inflexibility
- Use a questionnaire
  - To ensure proper documentation and uniformity in the due diligence process

©2010 Foley & Lardner LLP

Questionnaire Advantages

- Provides a uniform framework for due diligence
- Ensures "apples-to-apples" comparison of vendor responses
- Ensures all key areas of diligence are addressed
- Provides an easy means for incorporating due diligence information into the final contract

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Questionnaire Key Areas

- Financial condition
  - Example from ASP and hosting industry
- Insurance coverage
- Responsibility
  - Criminal convictions
  - Litigation
  - Regulatory enforcement actions
  - Breaches of security, health information
  - Adverse audits
  - Affiliates, Subsidiaries, contractors outside the US

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Questionnaire Key Areas

- Intended use of subcontractors
- Personnel Security
  - Screening procedures
  - Training
  - Ongoing education
  - Termination procedures
- Information Security Policy

©2010 Foley & Lardner LLP

Questionnaire Key Areas

- Intended use of subcontractors
- Personnel Security
  - Screening procedures
  - Training
  - Ongoing education
  - Termination procedures
- Information Security Policy

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Questionnaire Key Areas

- Development and Maintenance Procedures
  - Security controls during development lifecycle
  - Security testing
  - Separate environments for testing and production
- Privacy Policy

©2010 Foley & Lardner LLP

2. NDA or Confidentiality Clause

- NDA or Confidentiality Clause
  - Language should be broadly drafted to include all potential confidential information
- Marking requirements disfavored/unworkable
- Ongoing protection of trade secrets
  - Terms on NDAs have been held to limit trade secret protection

©2010 Foley & Lardner LLP

Standard of Care for Confidentiality

- Vendor shall treat Customer Confidential Information as strictly confidential and shall use the same care to prevent disclosure of such information as it uses with respect to its own most confidential or proprietary information, but in no event less than reasonable care.
- Vendor shall treat Customer Confidential Information as strictly confidential and shall use the same care to prevent disclosure of such information as it uses with respect to its own most confidential or proprietary information, **which shall not be less than the standard of care imposed by state and federal laws and regulations relating to the protection of such information and, in the absence of any legally imposed standard of care,** the standard shall be that of a reasonable person under the circumstances.

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

3. Warranties

- Compliance with best industry security practices
- HIPAA/HITECH compliance
- GLB compliance
- Red Flag/Identity Theft
- Other state and federal consumer protection/privacy laws
- Compliance with privacy policy
- Personnel not convicted of crimes of dishonesty
- Performance of services outside the US
- Transmission of confidential information outside the US

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

4. Use of Subcontractors

- Strictly limit
- Approval required
- Joint and several liability
- Due diligence
- Consider use of NDAs to achieve direct contractual privity
- Use of subcontractors to provide critical functions – hosting providers, outsourcing partners, etc.
  - Far greater need for due diligence
  - Potential use of a "continuity agreement"
  - Control over changes in these types of service providers
    - Ample notice of a change
    - Assistance in conducting diligence
    - Termination right

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Use of Subcontractors, continued

- For critical subcontractors, consider use of a specialized "Subcontractor NDA"
  - Creates privity of contract
  - Ensures that the subcontractor is on notice of obligations
  - Describes relationship between and among the parties
  - Where appropriate, include specific security requirements in addition to baseline confidentiality

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

5. Personnel Due Diligence and Control of Personnel

- Background checks and screening
  - Scope restricted by applicable law
  - Reassign personnel who fail required check
  - Reserve right to conduct your own check
- Control of Personnel
  - Ability to request removal of non-performing personnel or any personnel that present a security threat
  - Consistency of staff over the term of the project
  - Question vendor about turnover rates
  - Reserve right to fingerprint and search all items brought into or out of your facilities
  - Reserve the right to monitor and review all use of your systems by vendor personnel

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Control of Personnel, continued

- Control of Personnel
  - Compliance with facility access and security policies
  - Vendor identification card
  - Access scheduling
  - Escorts required
- General Audit Provision
  - Permit audit of vendor compliance with contract terms, including confidentiality, security, personnel, etc.
- No Removal of Data

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

6. General Security Obligations

- Take all reasonable measures to secure and defend its systems and facilities from unauthorized access or intrusion
- Periodically test systems and facilities for vulnerabilities
- Immediate reporting of breaches
- Joint security audits
- Regulatory access and compliance
- Firewalls, antivirus, use of VPNs, on-demand access
- Termination for compliance issues

©2010 Foley & Lardner LLP

7. Indemnity

- Indemnity -- Protection from third party claims
  - Breach of confidentiality
  - Failure to comply with security requirements

©2010 Foley & Lardner LLP

8. Limitation of Liability

- Exceptions to Limitation of Liability
  - Breach of confidentiality
  - Indemnity
  - Use of name
  - Misappropriation of intellectual property
- Termination for compliance issues

©2010 Foley & Lardner LLP

9. Security Breach Notification for PII Control of Costs

- Control of notice
  - Ensure prompt notice from vendor of actual or potential/suspected breach to ensure your company's ability to comply with applicable laws (i.e., avoid eleventh hour notices)
- Allocate responsibility for costs vendor

©2010 Foley & Lardner LLP

10. Insurance

- Workers Compensation
- Commercial General Liability
- Commercial Automobile
- Commercial Blanket Bond, including Electronic & Computer Crime or Unauthorized Computer Access coverage
- Professional Liability Insurance (Errors and Omissions)

©2010 Foley & Lardner LLP

11. Information Handling Requirements

- Where appropriate, attach specific information handling requirements in an exhibit
  - Securing PII
  - Encryption
  - Secure destruction of data
  - Securing of removable media
  - Communication and coordination

©2010 Foley & Lardner LLP

12. Additional Considerations

- Due Diligence Questionnaire
  - Attach as an exhibit and incorporate into the agreement.
  - Include means to be notified of material modifications to responses.
  - Ensure vendor will not materially reduce the security protections reflected in the Questionnaire.
- Annual certification of compliance

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Additional Thoughts

- One size does not fit all
- Importance of flexibility in the contracting process
- Develop a library of alternate "plug and play" contractual provisions to address common areas of disagreement

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Post-Execution Follow-up

- Ongoing policing of vendor performance and compliance is crucial
  - Audit rights
  - Access to third party audit reports (SAS 70 Type II)
  - Update due diligence questionnaire
- Annual compliance statement
- Ongoing reevaluation of contracting approach to reflect
  - Changes in laws and regulations
  - Feedback from vendors
- Developing means to address vendor feedback can speed negotiations and lower costs
- Contracting is a dynamic process

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

Questions?

Peter McLaughlin
Senior Counsel
Foley & Lardner
pmclaughlin@foley.com
(617) 502-3265

Matt Karlyn
Senior Counsel
Foley & Lardner
mkarlyn@foley.com
(617) 502-3231

©2010 Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP