Morgan Lewis

# Outsourcing in the Financial Services Industry

**March 22, 2012**

John Ayanian | Barbara Melby | Marc Stark | Peter Watt-Morse | Joe Zanko

www.morganlewis.com

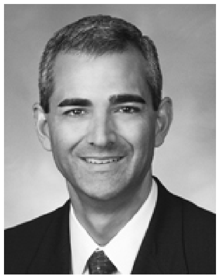
# Introduction

Please note that any advice contained in this presentation is not intended or written to be used, and should not be used, as legal advice.

# Agenda

- Introduction
- Industry Trends *(Marc Stark and Joe Zanko)*
- An Overview of the Regulatory Environment (*John Ayanian*)
- Identifying Key Security Issues *(Peter Watt-Morse)*
- Wrap-up and CLE information

# Participants




## John Ayanian
**Partner**
**Morgan Lewis**
P: 202.739.5946
Email: jayanian@morganlewis.com



## Barbara Melby
**Partner**
Morgan Lewis
P: 215.963.5053
E: bmelby@morganlewis.com



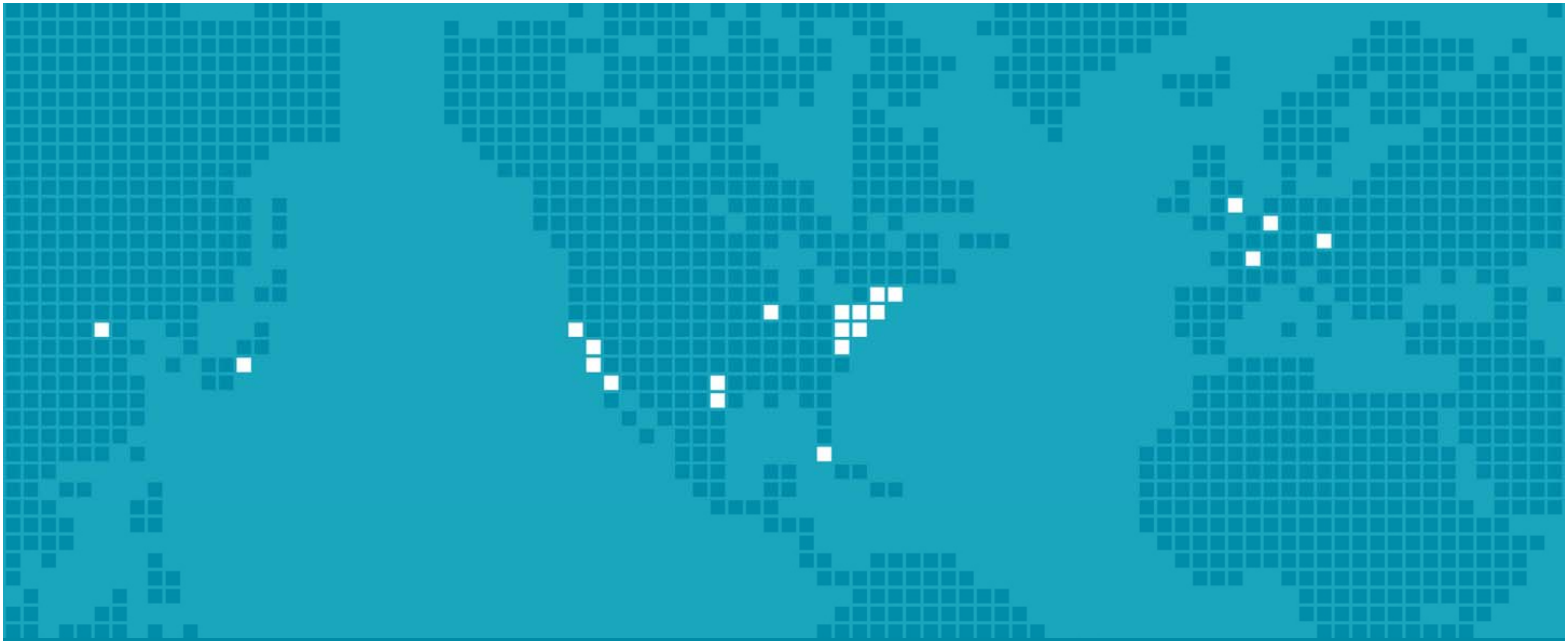
## Marc Stark
**Director**
KPMG
P: 917.375.9610
E: mastark@kpmg.com



## Peter Watt-Morse
**Partner**
Morgan Lewis
P: 412.560.3320
E: pwatt-morse@morganlewis.com



## Joe Zanko
KPMG
P: 908.403.0964
E: jzanko@kpmg.com



# Industry Trends

# Overarching Issues Impacting the Financial Services Industry

- Regulatory changes
  - Emerging FINRA Rules (e.g. 3190)
  - Dodd-Frank Act
  - Stricter capital requirements (e.g., Basel III)
- Market turbulence/uncertainty
- Continued margin pressures
- Overcapacity
- Continued industry contraction

# Key Services Trends by Segment

| Banking | Capital Markets | Insurance |
| --- | --- | --- |
| • Increasing regulatory scrutiny forcing core operational changes<br>• Difficult market conditions putting new pressure on operational efficiency<br>• Continued expansion of alternative operating models for horizontal process areas<br>• Continued expansion of alternative operating models for core operational areas | • Evolving regulatory requirements forcing operational changes<br>• Continued pressure on back and middle office operations to transform operating models and enable a lower cost, high-performance environment<br>• Profitability challenges due to excess capacity and increased capital requirements<br>• Increased adoption of outsourcing<br>• Continued evaluation of viability of captive operations | • Increased margin pressures pushing continued evaluation of alternative operating models<br>• Slow but continued expansion of alternative delivery models with horizontal process areas (Finance, HR)<br>• Financial pressures forcing continued adoption of alternative models for middle-office operations (claims, calls, underwriting)<br>• Intense competition and increased customer turnover |

# Financial Services Firms are Increasing Outsourcing in Response to Unrelenting Market Pressures

**Outsourcing gaining strength**

- **Investment banks are increasingly opting for a buy model to support their transactional processes, rather than housing them in their local or offshore centers**
- **This is primarily being driven by a need to lower costs by leveraging the scale of the outsourcing provider and its expertise and experience**
  - Two large financial institutions have recently sold off their captive centers in India to outsourcing providers and are purchasing services back under BPO arrangements
  - Several other institutions are in the process of outsourcing activities from their captive operations, or are in early planning stages

**More value-added work moving to captives**

- **As the SSCs mature, banks are now looking at moving more high-end, complex or analytical processes to their offshore centers, while they move more vanilla processes to third parties. Examples at several institutions include:**
  - Many institutions are adopting multigeography strategies (even, at times, with multiple sites in a single country)
  - One European institution uses its nearshore centers in the US and UK, to support any outages in its offshore centers
  - Banks are also mitigating risk by adopting multivendor strategies, moving toward a stable of vendors as opposed to a single partner

**Decreasing risk appetite makes banks adopt a multilocation strategy**

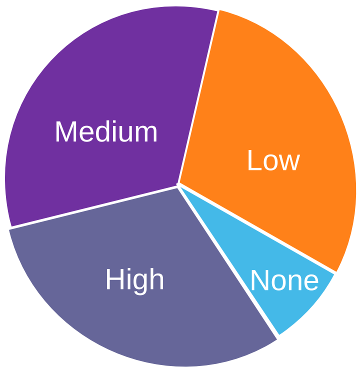
- **More banks are now spreading their operations across locations in an effort to decrease their dependence on certain geographies and ensure business continuity of processes**
  - Many institutions are adopting multigeography strategies (even, at times, with multiple sites in a single country)
  - One European institution uses its nearshore centers in the United States and UK to support any outages in its offshore centers
  - Banks are also mitigating risk by adopting multi vendor strategies, moving toward a stable of vendors as opposed to a single partner

# Shared Services and Outsourcing: Well-Established Methods for Managing SG&A Functions

## Shared Services has become the delivery model of choice…

Over 80% of Large Companies
Have Adopted Shared Services

Level Integrated Across Functions,
Geographies & Business Units

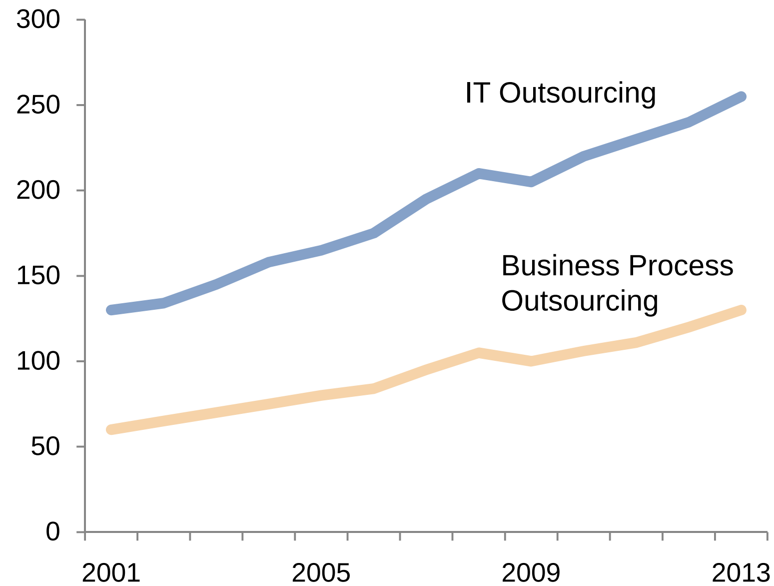



Of these, nearly two-thirds are operating in a model that is multifunctional and globally integrated

Source: Corporate Executive Board

## … with a growing portion of services delivered through outsourcing

Global Outsourcing Expenditures
($ B)




"Gartner on Outsourcing, 2009 – 2010," Gartner, Inc., December 23, 2009

# For Many Organizations, Their Approach into a Leveraged Service Model Follows a Traditional Maturity Life Cycle

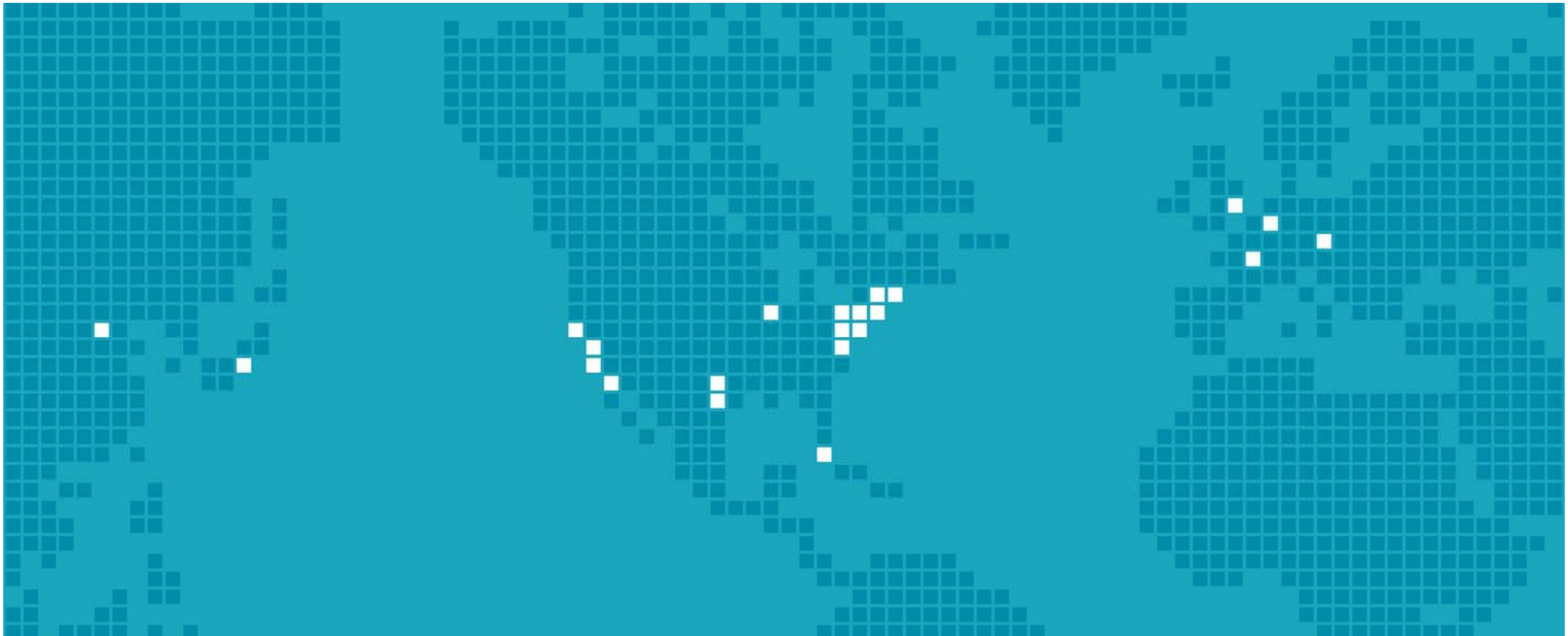
**Significant interest levels over the past 12 months suggest that the insurance segment, in general, is accelerating maturity**

| | | | | | |
|---|---|---|---|---|---|
| **Adoption Stage** | **Domestic Service Delivery** | **BPO Pilot** | **Scale** | **BPO as Key Element of Business Strategy** | **Transformed Global Operating Model** |
| **Characteristics** | • In-country operation only<br>• May include onshore outsourcing | • Initial offshoring steps<br>• Disparate initiatives | • Build on successful pilot<br>• Grow initial processes/functions<br>• Add new functions | • Expanded scope (strategic supplier relationships, captive, etc.) | • Offshore integrated as holistic part of global service delivery framework |
| **Examples** | No Global Delivery | Pilot/Education/ Proof of Concept | ROI/ Value Realization/ Risk Awareness | Strategic Supplier | Global Service Delivery |
| **Strategic Consideration** | Onshore | Cost saving | | Integrated Strategy/Transformation | |





KPMG



# An Overview of the Regulatory Environment

# FINRA Regulatory History

## NASD Notice to Members 05-48 – July 2005

– Primary focus on accountability and supervision

– Prohibitions on outsourcing certain "covered activities"

  - E.g., order taking, handling of customer funds and securities, and supervisory responsibilities

– A member may not "contract its supervisory and compliance activities away from its direct control"

  - "Does not preclude a member from outsourcing certain activities that support the performance of its supervisory and compliance responsibilities"

# Proposed FINRA Rule 3190

Background

- Clarify obligations and supervisory responsibilities
- Codify FINRA outsourcing guidance
- Require additional obligations for clearing and carrying members

# Proposed FINRA Rule 3190

General Requirements Applicable to All FINRA Members

- Continued responsibility to comply with applicable securities laws and FINRA and MSRB rules
- No delegation of responsibilities for, or control over, covered outsourced activities
- Supervisory system and written procedures for covered activities
- Registration and qualifications
- Ongoing due diligence requirements

# Proposed FINRA Rule 3190

Clearing and Carrying Firms

- Restrictions on outsourcing specified activities
- Oversight requirements
- Notifications to FINRA
- Exceptions

# Proposed FINRA Rule 3190

## Restrictions for Clearing and Carrying Firms

- A clearing or carrying member shall “vest” an associated person of the member with the “authority and responsibility” for:
  - The movement of customer or proprietary cash or securities;
  - The preparation of net capital or reserve formula computations; and
  - The adoption or execution of compliance or risk-management systems.



Morgan Lewis

# Proposed FINRA Rule 3190

Clearing and Carrying Firms Must Adopt Procedures to:

- Enable the firms to take "prompt corrective action" to achieve compliance with applicable securities laws and FINRA and MSRB rules
- Approve transfer of third-party service provider duties to a subvendor

# Proposed FINRA Rule 3190

Notification Requirements for a Clearing or Carrying Member

- Must notify FINRA of outsourcing agreements with third-party service providers and subvendors “to perform any function or activities related to the member's business as a regulated broker-dealer” within 30 days of entering into the agreement
- Within three months of rule adoption, must notify FINRA of all such outsourcing arrangements in effect as of the rule’s effective date



Morgan Lewis

# Proposed FINRA Rule 3190

Notification must include:

- Functions being performed by a third-party service provider (and subvendors if known)
- Identity and location of the third-party service provider (and subvendors if known)
- The identity of the third-party service provider's regulator (if any)
- A description of any affiliation between the firm and the third-party service provider

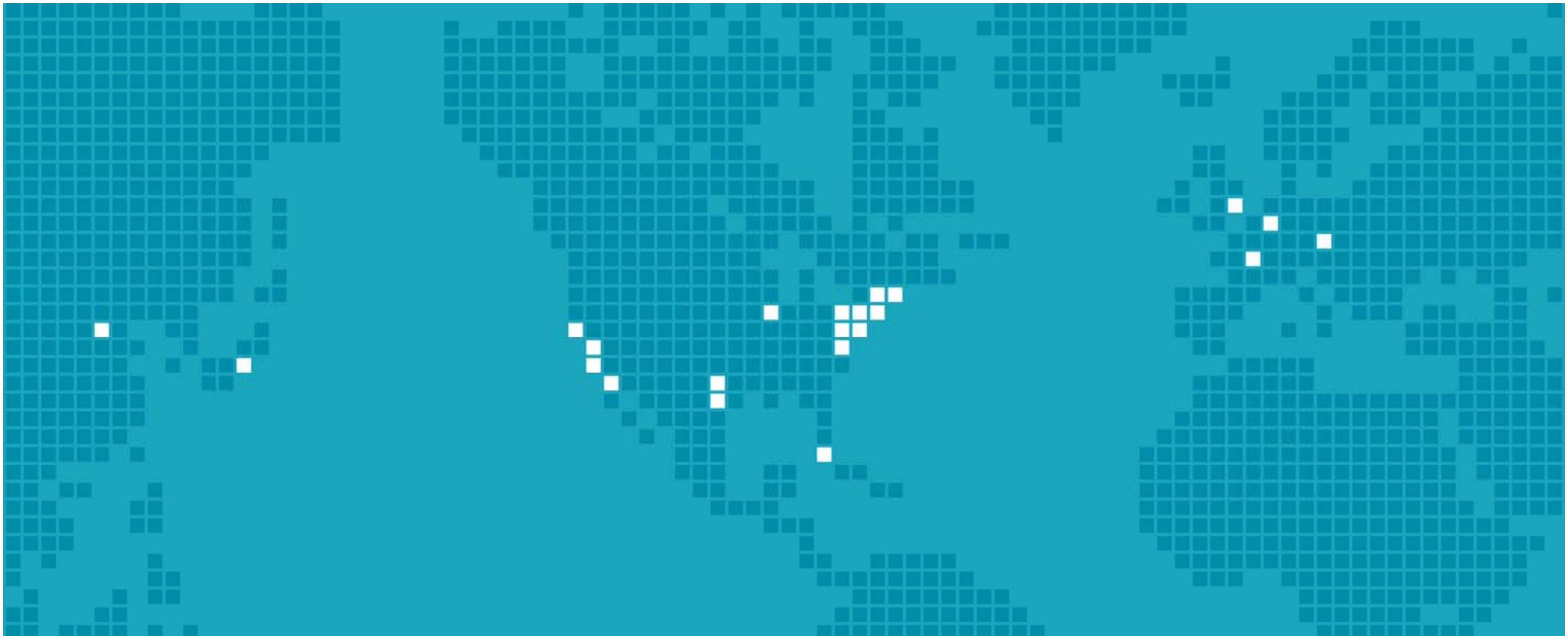
# Proposed FINRA Rule 3190

Exceptions:

- Ministerial activities
- Carrying agreement approved under FINRA Rule 4311

# FINRA Regulatory Notice 11-14

## Status of Rule Proposal



# Identifying Key Security Issues





Morgan Lewis

# Security: Key Outsourcing Issue

- Regulatory Requirements
- Potential Damages
  - Amount of Damages vs. Service Costs
  - “Customer Relation” Payments
  - Cost of Corrective Measures
- Reputational Risk

# Regulatory Background

- Federal Reserve
  - Federal Reserve Bank of New York:
    - *White Paper*
      - Independent validation of security processes
      - Responsible for management
  - Federal Reserve Board (FRB):
    - *Supervisory Letter*
      - Institutional controls for security are at least equivalent to internal controls

# Regulatory Background

- FDIC
  - Guidance:
    - *Structure agreements to protect against internal and external security threats*
  - Recommendations:
    - *Due diligence/risk assessment*
    - *Monitoring/audit*
    - *Termination rights*

# Regulatory Background

- Examinations – OCC, OTS, FFIEC
  - Compliance with Section 501 of Gramm-Leach-Bliley
    - *Comprehensive information security program to safeguard nonpublic personal financial information*
  - Security Guidelines:
    - *Outsourcing agreement includes all requirements contained in customer's internal written information security program*
  - Information Access:
    - *Transparency*
    - *Limits on service provider*

# Due Diligence

**Vendors:**

***"Don't worry – our security protections are adequate":***

- ✓ ***"We will provide you the same protection we provide for our own information"***
- ✓ ***"We are regulated and those regulations protect you"***
- ✓ ***"You cannot review our internal procedures based on confidentiality/security concerns"***





Morgan Lewis

# Due Diligence

**Understand the what, where, who, and how**

- ✓ **What** is the security offering vs. **What** are the security requirements?
- ✓ **What** types of data will be processed/hosted?
  - Nonpublic personal information (NPPI), business-sensitive information
- ✓ **Where** are the services being provided?
- ✓ **Who** is providing the services?
- ✓ **How** is data segregated and used?
  - May vary by environment (production, DR, backup, archive)

Work with Security, Audit, Risk, DR, Compliance

# Due Diligence

- Importance of getting respective teams together
  - Early in due diligence process – contract and exhibit documents align with discussions
- Comparison of security policies:
  - Meeting or exceeding internal security
  - Bridging the gaps
  - Attachment to contract
- Complete independent risk assessment

# Contract Provisions – Confidentiality

- Confidentiality Provisions:
  - Important but not sufficient – need process standards, monitoring and management, breach response
  - Issues:
    - *Vendor Sensitive Information – balancing transparency/vendor confidentiality*
    - *Segregation of Data – access and third-party information*

# Data Protection

- Ownership of Data
- Limitations on Other Uses
- Storage
  - Backup
  - Access
  - Return
- Record Retention
  - Policy alignment
  - Litigation holds/regulatory requirements
  - Destruction protections

# Data Protection

- Changes to Security Policies
  - Regulatory Requirements (e.g. PCI)
  - Customer-Initiated
    - *Change management process*
  - Vendor-Initiated
    - *No negative impact on security*
    - *Advance notice/documentation – compliance*
    - *Cost issues*



Morgan Lewis

# Data Protection

- Customer Data (NPPI)
  - Compliance with GLBA
    - *Compliance required of subcontractors*
    - *Ensure proper disposal of NPPI*
    - *Provide notice and information regarding breach, including payment for resultant credit monitoring services*
  - Fair Credit Reporting Act (Red Flags)
  - Massachusetts Regulations
    - *3/1/12 – Certification*

# Audit

- Who Conducts Audit?
  - Existing Internal Processes – Independent Auditors
- Frequency
  - Annual Plus
    - *Breaches*
    - *Policy Changes*
- Vendor Audits
  - Right to Notice of Results
- Regulatory Requirements
- SSAE16

# Subcontractors

- “Permitted Subcontractors”
  - Right of Approval/Customer Data
- Standards
  - GLBA Compliance
- Revocation
  - Regulatory Issues
  - Change Management
- Audit Rights



Morgan Lewis

# Remote Workers

- Worldwide mobile worker population will grow to 20% of workforce (1.19 billion people) by the end of this year
- Review internal policies
  - Laptops, mobile devices, noncompany devices, network connections
- Align vendor policies
  - Passwords, monitoring requirements, antivirus software, local storage, encryption, incident management
- Monitoring/future modifications





Morgan Lewis

# Data Breach

- Requirements for Notice
  – Security vs. Data Breach
  – Investigation/Transparency/Participation
- Remediation
  – Remedial Plan – Acceptance Testing
  – Change Management





Morgan Lewis

# Data Breach

- Liability
  - Cap Issues
    - *Costs of investigation/notification/monitoring excluded from cap*
  - Consequential Damages
    - *Primary damage*
    - *Exception to exclusion*
    - *Nonexcluded but capped*

# international presence

Beijing Boston Brussels Chicago Dallas Frankfurt Harrisburg Houston Irvine
London Los Angeles Miami New York Palo Alto Paris Philadelphia Pittsburgh
Princeton San Francisco Tokyo Washington Wilmington