

ACORD LOMA Insurance Systems Forum

Regulatory Updates

*Walt Disney World Dolphin,
Lake Buena Vista, FL
May 22-24, 2005*

Patrick J. Hatfield
Jon A. Neiditz
Lord, Bissell & Brook LLP
1170 Peachtree Street
Suite 1900
Atlanta, GA 30309
404-870-4684
phatfield@lordbissell.com
jneiditz@lordbissell.com



Agenda

- Intro's
- Privacy and Security
- Outsourcing laws
- e-Records and e-Discovery
- CAN-SPAM
- Telemarketing Laws
- Web Sites
- Summary
- Q&A



Privacy & Security

Outsourcing Laws

e-Records

CAN-SPAM

Telemarketing laws

Web Sites

Introduction

- Pat Hatfield
- Jon Neiditz
- Part of larger Lord, Bissell & Brook team covering these and related topics



Privacy & Security

Outsourcing Laws

e-Records

CAN-SPAM

Telemarketing laws

Web Sites

Introduction cont'd

- Objective - Raise your awareness of some significant developments and trends requiring collaboration among members of a multi-disciplinary team responsible for e-risks.
- Objective - For vendors in the room, raise your awareness of these topics so you revise your form agreements to address these concerns when dealing with insurers.



Privacy Laws

- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act and FACT Act
- Health Insurance Portability & Accountability Act
- Telemarketing and Consumer Fraud Protection Act and Telephone Consumer Protection Act
- CAN SPAM Act
- Privacy Act of 1974
- NAIC 1982 and 2000 Model Privacy Laws
- USA Patriot Act
- Laws re: Event Data Recorders, SSN, AIDS, Mental Health, Substance Abuse, Domestic Violence, Genetic Testing....



Privacy & Security

Outsourcing Laws

e-Records

CAN-SPAM

Telemarketing laws

Web Sites

Privacy - Overview

- ChoicePoint summary
- Reaction to the “ChoicePoint episode”
 - federal laws remain a possibility
 - states are enacting laws - AR, GA for example with more states to follow
 - objective of these laws will be to require more and more companies - not just ChoicePoint and other consumer reporting agencies, to monitor for breaches and notify consumers



GLBA Privacy for Insurers

- GLBA applies to “financial institutions” - including insurers and insurance agents
- The National Association of Insurance Commissioners (NAIC) developed the influential model for state legislatures.
- 1982 NAIC Model Privacy Law (17 states)
- 2000 NAIC Model Privacy Regulation
 - Almost all states have adopted, but some have significant deviations and others may follow



GLBA Privacy

Regulation of Nonpublic Personal Information:

- Nonpublic Personal Financial Information (NRFI)
 - Opt-Out Model
 - 3 Basic Exceptions
- Nonpublic Personal Health Information (NPHI)
 - Opt-In Model
 - Various exceptions



Security - Overview

- Security Laws
- States expanding on security



Privacy & Security

Outsourcing Laws

e-Records

CAN-SPAM

Telemarketing laws

Web Sites

Security Laws

- HIPAA Security
- GLBA Safeguards
 - Federal and state laws
 - Spreading beyond financial institutions under FTC's broad consumer protection powers
- California SB 1386 -- Spreading to other state and federal laws courtesy of ChoicePoint
- California AB 1950
- FACTA Disposal Rule
- Sarbanes-Oxley
- EU Data Protection and its progeny



Universal Information Security Issues

- Administrative Security
 - Program definition & administration
 - Managing workforce risks
 - Employee training
- Technical Security
 - Computer systems, networks, applications
 - Access Controls
 - Encryption
- Physical Security
 - Facilities
 - Environments safeguards
 - Disaster recovery

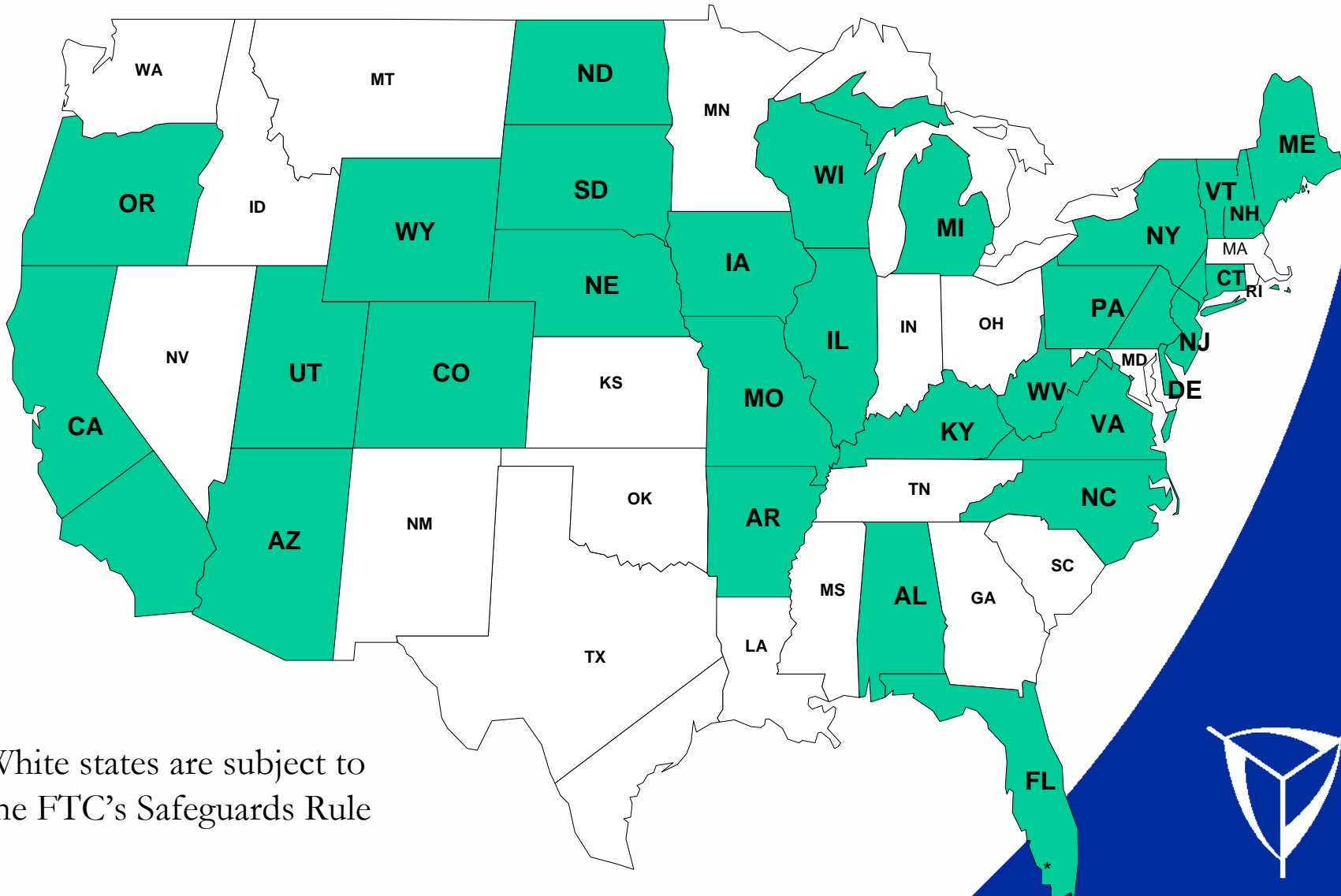


GLBA Safeguards Rule (FTC)

- Financial institutions must implement “reasonable security,” a written program that is appropriate to:
 - the company’s size and complexity,
 - the nature and scope of its activities, and
 - the sensitivity of the customer information it handles.
- As part of its program, each financial institution must:
 - assign one or more employees to oversee the program,
 - conduct a risk assessment;
 - put safeguards in place to control the risks identified in the assessment and regularly test and monitor them;
 - require service providers, by written contract, to protect customers’ personal information; and
 - periodically update its security program.



States that Have Adopted GLBA Safeguards Laws



White states are subject to the FTC's Safeguards Rule



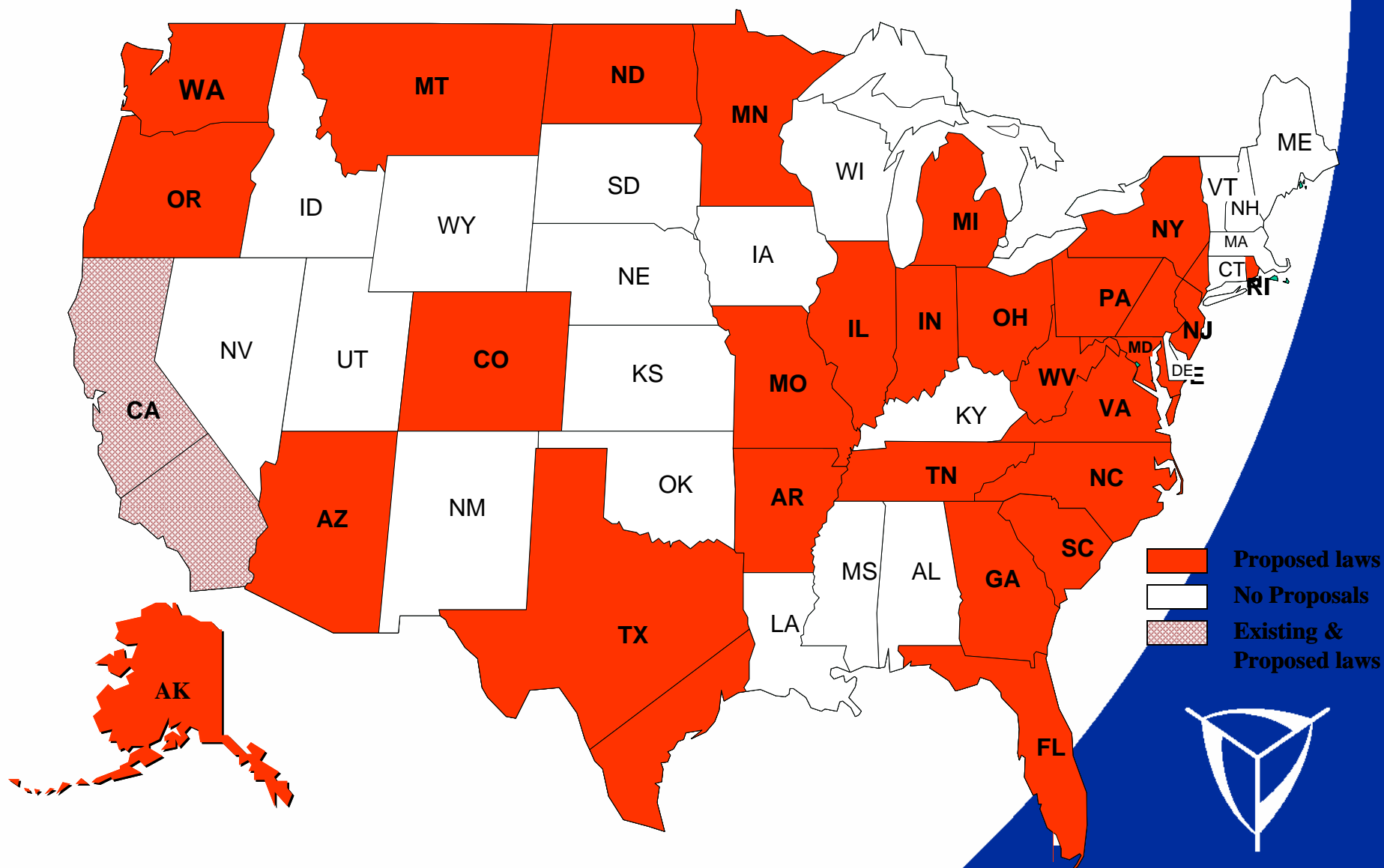
- Privacy & Security
- Outsourcing Laws
- e-Records
- CAN-SPAM
- Telemarketing laws
- Web Sites

California: Notification of Breaches

- SB 1386
 - Effective since July of 2003
 - Requires firms that conduct business in California to notify California consumers of security breaches that may have compromised the integrity or confidentiality of their computerized personal information
 - Compliance (at first) only for Californians by ChoicePoint will lead to its adoption in other states, and perhaps nationally
 - May have already become a national standard of care
 - Treat it as such to avoid potential liability, but more importantly loss of customer and public trust



State Security Breach Bills



Elements of the Strongest Bills (Supported by AG Spitzer)

- Security freezes on credit files
- Increased protection against companies disclosing Social Security numbers
- Consumer notice whenever a company shares personal data with another party, as well as of security breaches
- Access to profiles
- Enabling criminal complaints with law enforcement agencies, and tougher criminal penalties, including on use of encryption to conceal a crime
- Opt-out list for consumers who do not want their personal data shared



FCRA and FACTA

- More than just credit reports
- These laws apply to insurers in a variety of ways
- Disposal of Information



FACTA's Rule on HOW to Dispose

- Compliance date June 1, 2005
- Disposal of consumer report information under FCRA
- FACTA (2003) responded to identity theft-related concerns
- “Consumer information” under FACTA includes records:
 - that are consumer reports, or
 - are derived from consumer reports
- Requires due diligence and monitoring of entities contracted to dispose of consumer information.
- Flexible and scalable.
- For WHEN to dispose, consult your NEW record management program



California: Spreading “Reasonable Security”

- AB 1950
 - Effective since January 1, 2005
 - Requires businesses that “own or license” personal information about California residents to implement and maintain reasonable security practices, and require their contractors to do the same
 - Written to apply to organizations not previously covered by security requirements, specifically including HIPAA but not GLBA
 - Deems compliance with any law “providing greater protection” sufficient
 - Dovetails with FTC’s expansion of the GLBA Safeguards standards to non-financial entities



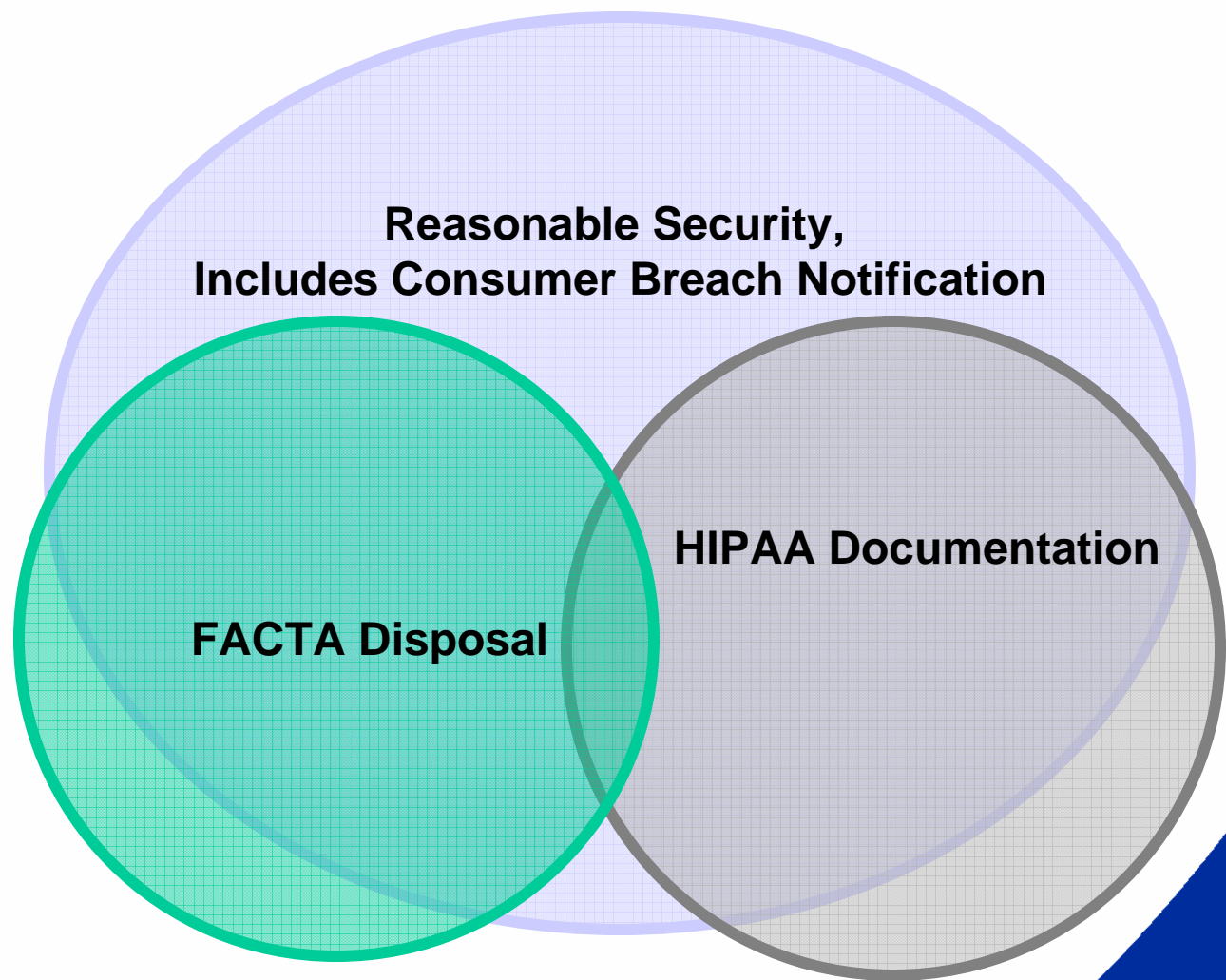
**Other information security laws care less about whether the entity is covered,
and more about the nature of the information.**

Law	Type of Information Protected	Source or Holder of Information
HIPAA	PHI is anything that could identify a person (and some things that arguably could not)	Created or received by a covered entity
FACTA	<ul style="list-style-type: none"> •“Consumer information” includes any record about an individual, in any form, that is a consumer report or is derived from a consumer report •“Consumer report” is any communication by a consumer reporting agency bearing on credit-worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, that is to be used for purposes including personal credit, insurance or employment. •“Consumer reporting agencies” include many entities that regularly furnish information on consumers 	ANY entity possessing consumer information (although that information must be derived from information generated by a consumer reporting agency)
CA SB 1386	<p>First name or first initial and last name in combination with any of the following data elements, when either the name or the data elements are not encrypted:</p> <ul style="list-style-type: none"> (1) Social security number, (2) Driver's license # or California ID Card # (3) Account #, credit or debit card #, in combination with any required code or password that would permit access to an individual's financial account 	Any entity doing business in CA that owns or licenses computerized data including personal information

Using HIPAA as the most specific set, compare requirements across laws.
 For example, here is a comparison regarding third party contracts.

HIPAA Imp. Spec	FTC GLBA Safeguards Rule	NAIC Model Regulation 673	State Variations to NAIC Model Regulation	Other Laws (FACTA & State Laws)
<p>Written Contract or Other Arrangement - Document the satisfactory assurances required through a written contract or other arrangement with the BA that meets the applicable requirements for BA contracts in §164.314(a).</p>	<p>Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards. 16 CFR § 314.4(d).</p>	<p>Exercise appropriate due diligence in selecting its service providers; and B. Require service providers to implement appropriate security measures, and, where indicated by the risk assessment, take appropriate steps to confirm that service providers have satisfied these obligations. Section 8.No contract requirement</p>	<p>AK - Not specifically addressed ARK - Not necessary for licensee to confirm service providers have satisfied obligations. CT - absolute requirement to confirm service providers have taken appropriate steps. KY - Not specifically addressed NC - Not specifically addressed ND - Licensee must obtain “satisfactory assurances from the service provider that it will appropriately safeguard the information.” VA - Not specifically addressed</p>	<p>Cal Civ Code § 1798.81.5(c) - A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction use, modification, or disclosure.</p>

Shape of an Information Security Program (particularly after the ChoicePoint incident)



Sarbanes-Oxley Impact

- Compliance with the various privacy/security laws has ongoing impact on overall compliance program, triggering Sarbanes-Oxley implications which in turn impact scope of audits conducted by internal and external auditors



Privacy and Security - Overview

Now what?



Privacy & Security

Outsourcing Laws

e-Records

CAN-SPAM

Telemarketing laws

Web Sites

Privacy and Security - Take-Away

- Unlike when the privacy requirements were hottest, you can now implement security in an efficient “once-and-done” approach
- still requires on-going monitoring changes in laws, risks and IT



Privacy and Security - Take-Away, cont.

- Evaluate not only the company's own infrastructure, but consider which suppliers/customers need to be included as well
- Evaluate compliance by company's agents and other significant intermediaries



Privacy and Security - Overview

- vendors - be prepared for more demands in this area from your customers
- companies who outsource - obligate your outsourcers to comply and monitor and report compliance, as well as let you verify compliance



Outsourcing Laws Update

- Foreign outsourcing concerns remain, event post-election
- 10 states had legislation introduced regarding foreign call centers
- 14 states had legislation introduced regarding sensitive information transmitted offshore
- State contracts - may require all services performed in that state or within U.S.
- BPO outsourcing - Reminder that some BPO deals may require a TPA license, claims adjuster license or require some other license



Let's Start with Biggest Risks

Insurance Carriers and Business Partners On The Hotseat?

**INSURANCE OFFICER
PLEADS GUILTY**

**AIG: Fires 2 Top Executives
as Probe Intensifies**

**BANK OF AMERICA BEGINS FIRING EXECUTIVES
TIED TO SPITZER PROBE**

**Marsh, ACE charges seen as
limited, but more suits
promised**

**AIG may have up to \$3B in
accounting mistakes**

**AON DOCUMENT SUGGESTS
WIDER SPITZER PROBE**



e-Discovery - A Few Basics

- plaintiffs and regulators getting more savvy about searching emails for the “smoking gun”
- Morgan Stanley case involving very expensive sanctions for not turning over all the emails
- while the storage cost drops, the cost of effectively searching and sorting rises, and the cost of being wrong also rises



Emails Are or Will Be the Focus of All These Investigations

- The New York AG's Office considers email "the functional equivalent of eavesdropping"

(Source: "Inside Eliot's Army, New York Magazine, January 10, 2005)

- "Lawyers used to say that the great engine of truth is cross-examination, and that's how they found out what really happened. But today it's email -- that's where people put their most unguarded, and often their most damaging, thoughts down. There's no way to do these cases except to read the e-mails."

(Source: *David D. Brown IV, Chief of Eliot Spitzer's Investment Protection Bureau, NPR Marketplace Interview, December 10, 2004*)



Privacy & Security

Outsourcing Laws

e-Records

CAN-SPAM

Telemarketing laws

Web Sites

Is Your Records Management System Obsolete?

- By the end of 2006, 60 billion email messages will be sent daily
- 60% of business-critical information is stored within corporate email systems (i.e., in unstructured data), up from 33% in 1999
- Fewer than a third of electronic documents are ever printed

(Source: Kenneth J. Withers and UC Berkeley)



Your Records Management Program Now

- In any records management program, data elements are classified based on:
 - Sensitivity and privacy (use and disclosure rules)
 - Country of origin
 - For U.S. data, specific retention, destruction, storage and other compliance requirements
- Company employees and managers should also be classified – permitting access to data based on roles.
- These two classification systems can create greater risks than they mitigate in view of unstructured data and the prosecutorial engine it feeds, as well as end-user compliance issues.



Suggested Questions for Your New Records Management Program

- First of all, have you considered every approach and adopted a good strategy to prevent your employees from creating the emails that will do you in?
- How many litigation or investigation obligations can you predict?
- Has relevant data been properly identified and preserved?
- What is the time, difficulty and cost (including business disruption) to recover and retrieve relevant data?
- How can costs be managed to avoid skyrocketing costs for future requests?



Zubulake IV

- *Zubulake IV* established responsibilities for legal counsel to monitor the preservation process. These responsibilities include:
 - That all relevant information and its sources must be identified
 - That relevant information is retained on a continuing basis
 - That relevant non-privileged material is produced to the opposing party in response to proper discovery demands



Zubulake V

- *Zubulake V* provides instructions for counsel to follow as a means of demonstrating their “continuous efforts” to preserve and avoid spoliation. These responsibilities include:
 - Issuing a litigation hold
 - Communicating directly with key players in the litigation and clearly communicate their preservation responsibilities
 - Instructing all employees to produce electronic copies of relevant active files
 - Ensuring all required backup media is identified and stored in a safe place



Your Old 30, 60, 90-day Email Destruction Policies

- Email destruction policies often driven by storage capacity considerations, not business or compliance needs
- Assure that all preservation exceptions, predictable and unpredictable, are met
- If you can't guarantee destruction of all copies, you have retained it
- Check how often your backup tapes are overwritten



2004 ARMA Survey: E-Records

- 2,200 record managers surveyed
- 47% -electronic records not included in company retention policy
- 46% -no system for suspending destruction of records for pending litigation or regulatory investigations
- 65% -litigation hold policy does not include electronic records
- 71% -IT department oversees retention of electronic records



2004 ARMA Survey: Email

- 840 U.S. businesses surveyed
- 21% had email subpoenaed in a lawsuit or investigation, up from 11% in previous year
- 13% defended lawsuits triggered by employee email, up from 4% in previous year
- 35% have written email retention policies



e-Discovery - Take-Aways

- Technology will play a big role in devising more robust record retention/purge policy and for monitoring compliance
- As e-business increases, so will relevance of all the e-records
- Consider how to assemble multi-disciplinary team for more effective e-records management process, including unstructured data, before the subpoenas arrive



CAN-SPAM ACT UPDATE

Primary Purpose Rule

- “Final Rule: Defining What Constitutes a Commercial Electronic Mail Message”
 - Specific criteria to be used to determine the primary purpose of an email message for purposes of regulation under the Act.
 - Effective March 28, 2005
 - Defines two types of messages
 - Commercial Electronic Message (CEM)
 - Transactional or Relationship Message (TRM)



Challenge Under CAN-SPAM Rule

- Application of the “message body interpretation criteria”
- FTC proposing amending regulation
 - no fee or other quid pro quo for opt-outs
 - P.O. and private mail boxes acceptable
 - clarify definition of “sender” who is responsible for compliance
 - shorten 10 day opt-out to 3 days



State SPAM Laws Updates

- CA, FL, MD (ruled unconstitutional), MI & UT passed laws in 2004
- VA won first criminal case in 2004
- More state legislatures considering in 2005



Telemarketing Laws Updates

- New FTC rule requiring DNC list scrub every 31 days, effective January 1, 2005
- IN & WI fighting FCC federal preemption of existing business relationship (EBR)
 - IN- customer calls only with “express permission”
 - WI- one call to customer
- FL- rule banning pre-recorded telemarketing calls to customer



Contrasting DNC and CAN-SPAM

- No “primary purpose” test for telemarketing
- No EBR exception for spam
- You cannot go to jail for DNC violation
- State Insurance Departments have enforcement authority for spam, but not DNC



Website Reviews

- Web sites are getting more interactive, therefore of more interest to plaintiffs and regulators
- There are a variety of laws that apply to web sites promoting insurance
 - privacy
 - insurance advertising
 - licensing status
 - FTC reviews
- Consider which linked sites should be reviewed



Wrap-Up

- These are complex topics - we only skimmed the surface
- Insurers - if you outsource any of these items, confirm that your contracts deal with the topics appropriately, don't assume vendors know these laws
- Vendors - the trend of addressing compliance topics (privacy and security for example) will continue - consider addressing topics head-on in your forms as a way to exhibit industry knowledge (and risk mitigation)



Questions? and Answers!

