When HIPAA is Just One of Many Information Security Challenges:

Integrating HIPAA Security with FACTA Disposal, GLBA, California, European and Other Requirements

HIPAA Summit 10

April 6, 2005

Jon Neiditz and Pat Hatfield

jneiditz@lordbissell.com

phatfield@lordbissell.com

LORD BISSELL BROOK LLP

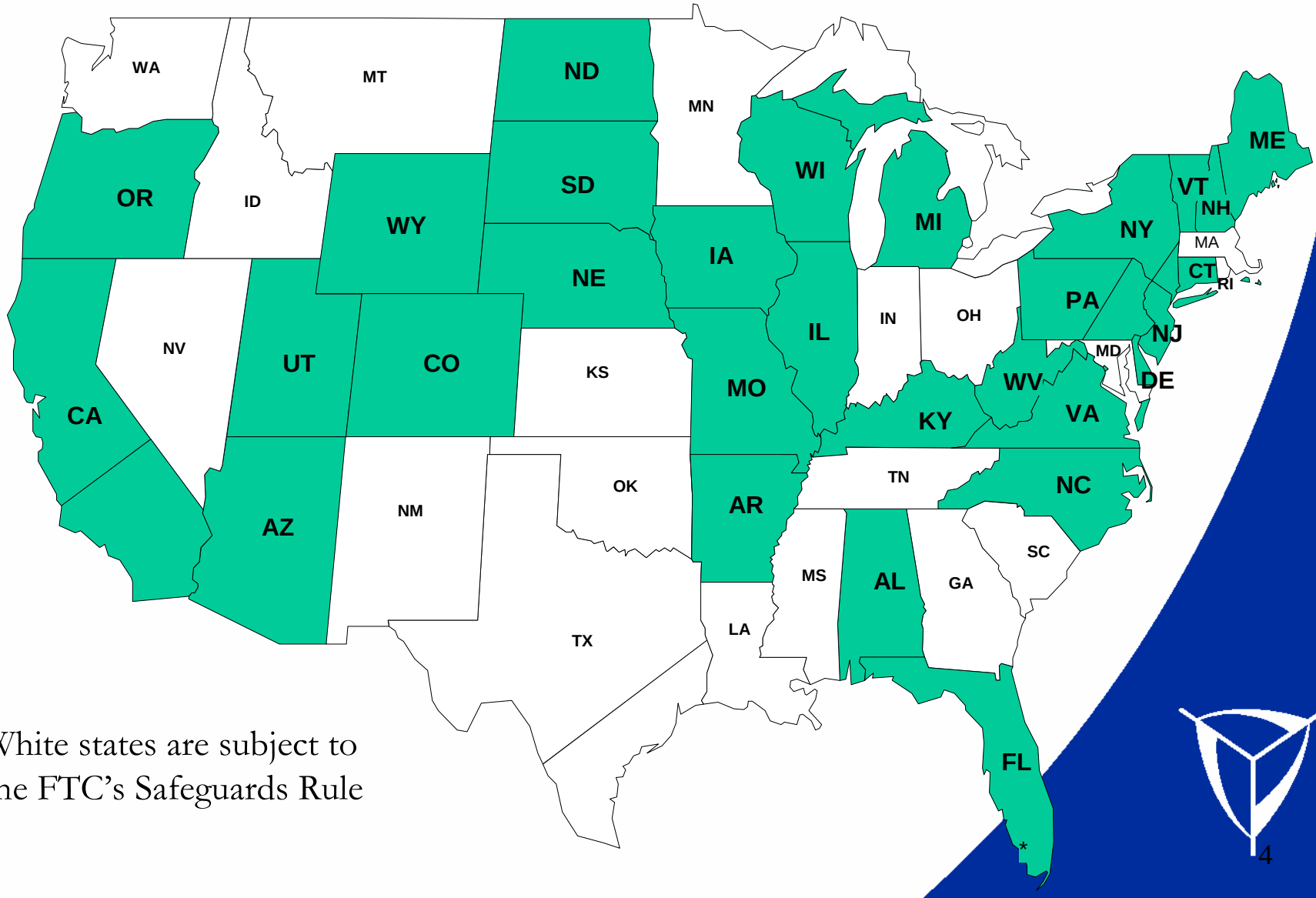
Layers of Laws

- 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

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

California Law 1

- 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

California Law 2

- SB 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

The FACTA Disposal Rule

- Compliance date June 1, 2005
- Disposal of consumer report information under FCRA
- FACTA (2003) responded to identity theft-related concerns
- "Consumer reports" under FCRA broadly defined:
  - "credit-worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living"
- "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.
- Explicitly designed to mirror the "reasonableness" standard of the Safeguards Rule.
- Flexible and scalable.

Classifications of Data and Access

- Data elements should be classified based on:
  - Sensitivity (e.g.,SSN, medical data)
  - Country of origin
  - For U.S. data, specific retention, destruction, storage and other compliance requirements (e.g., data collected for EEOC compliance)
- Company employees and managers should also be classified – permit access to data based on roles
  - Company directory may available to all, but SSN on a need-to-know basis
  - Special controls on data related to, e.g., performance reviews, workplace investigations

But Even with the Best Classification…

- The great, ultimately insurmountable challenges are:
  - Unstructured data (e.g., emails) and
  - End-user compliance
- What will courts determine to be reasonable for a company to retain, monitor, prevent and produce?
- Consider the dilemmas almost all companies face in the area of records management….

The Logic of Records Disposal 1

- FACTA's Disposal Rule is clear that it does not require the destruction or maintenance of any document, nor does it alter any such requirement.
- Those requirements will be driven by statutory record retention requirements, statutes of limitations, business needs and litigation risks.
- A records management program is necessary in order to establish defensible and efficient rules for the destruction of documents.
- But these rules must be subject to perpetual exceptions, and frequently suspended….

The Logic of Records Disposal 2: Sarbanes-Oxley

- The regular destruction of documents must be subject to suspension
  - to prevent spoliation of evidence
  - to comply with Section 802 of the Sarbanes-Oxley Act, which has been interpreted to prevent destruction or alteration of documents that could be subject to a federal investigation in the future.
- Some organizations are finding their information security controls meet Sarbanes-Oxley materiality requirements, subjecting those controls to audit and testing.
- Audit and testing under Sarbanes-Oxley is often a higher standard than “reasonable security” under GLBA or FACTA

The Logic of Records Disposal 3

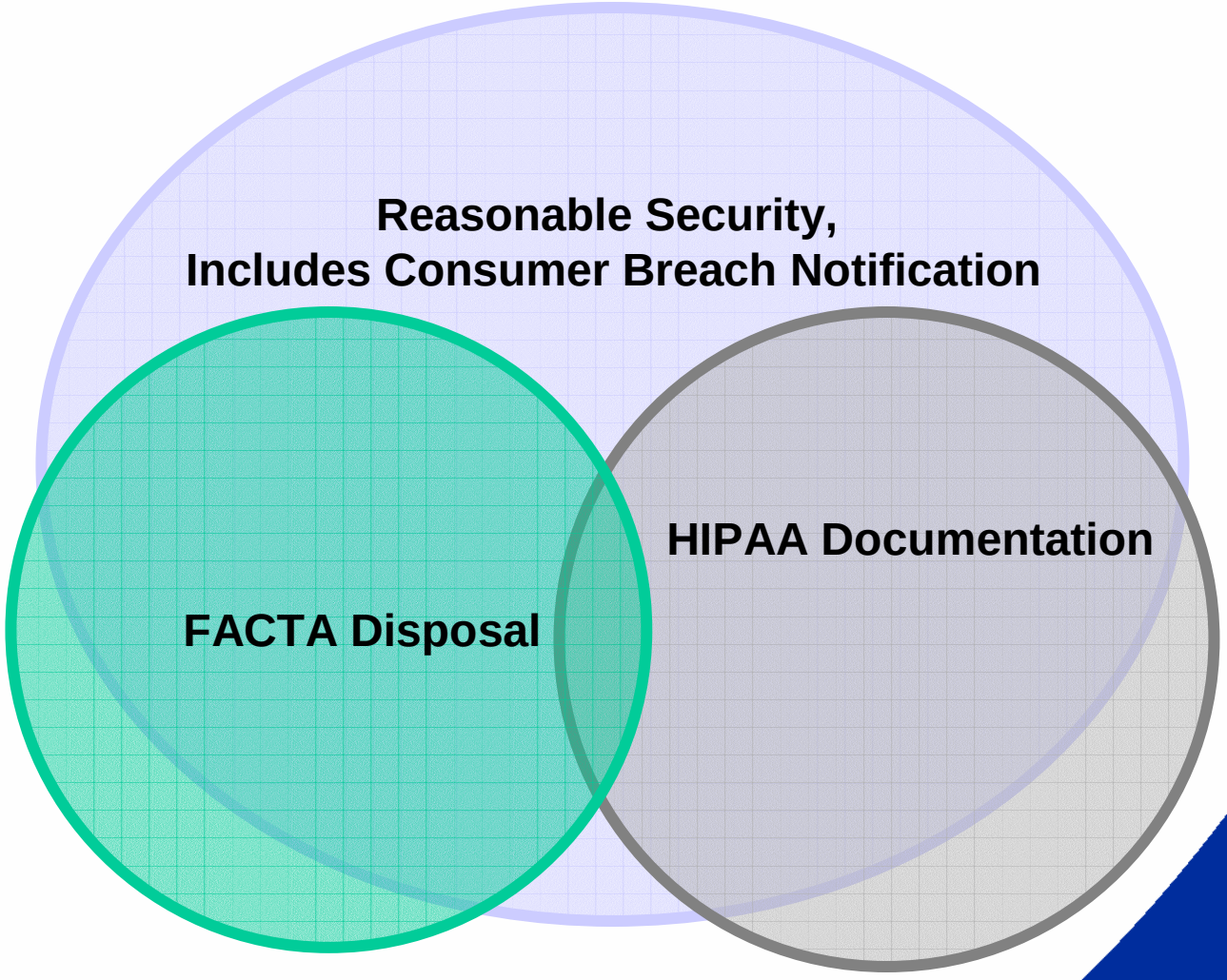
- No document management system will ever capture all documents subject to content-specific retention and production requirements, including
  - sectoral regulation,
  - prospective litigations/investigations, and
  - e-discovery
- Organizations need the ability to search through unstructured data, including emails and PDFs.
- Zubulake IV and V have begun to establish the standard that organizations must meet.
- Practice and technology must catch up.

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	•"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	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: (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)
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).	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).	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	**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	**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.

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



The Global Employer's Challenge

US-EU Comparison

- US gives rights to EMPLOYERS
  - Security concerns predominate
  - Continuous and multi-dimensional employee monitoring
  - Aggressive background checks permitted (& increasingly required)
  - Employee expectations of privacy are very limited
- EU gives rights to EMPLOYEES
  - Privacy concerns predominate
  - Monitoring only permitted with specific and limited legal justification
  - Limited background checks
  - Employees have broad privacy expectations and rights

Questions?

Jon Neiditz
Pat Hatfield
Lord, Bissell & Brook LLP
1170 Peachtree Street
Suite 1900
Atlanta, GA 30309
404.870.4600
jneiditz@lordbissell.com
phatfield@lordbissell.com