

Draft

CREF07

MBA's CREF/MULTIFAMILY HOUSING CONVENTION & EXPO
MANCHESTER GRAND HYATT SAN DIEGO • SAN DIEGO, CALIF.

FEBRUARY 4-7 **2007**

International, Offshoring and other Trends

Moderator:

Erin E. Stafford, Senior Vice President-CMBS, Dominion Bond Rating Service

Panelists:

Ken N. Beyer, President, Global Real Estate Services, OfficeTiger

Dave J. Bodi, CMB, Executive Vice President, Midland Loan Services, Inc./PNC Real Estate Finance

Ronald Lafever, Managing Director, Johnson Capital International

Lisa J. Sotto, Partner, Hunton & Williams, LLP

**HUNTON &
WILLIAMS**

Draft

CREF07

MBA's CREF/MULTIFAMILY HOUSING CONVENTION & EXPO
MANCHESTER GRAND HYATT SAN DIEGO • SAN DIEGO, CALIF.

FEBRUARY 4-7 **2007**

The Privacy Implications of Outsourcing: Defining the Issues

Lisa J. Sotto

Partner

Hunton & Williams, LLP

(212) 309-1223

lsotto@hunton.com

**HUNTON &
WILLIAMS**

Hunton & Williams

- Founded in 1901, Hunton & Williams is one of the nation's leading law firms with 900 attorneys in 18 offices, serving clients in over 100 countries
- 20 privacy professionals in the U.S., EU and Asia
- Our privacy clients include:
 - Pitney Bowes
 - GE
 - General Dynamics
 - Holtzbrinck Publishers
 - Polo Ralph Lauren
 - Estee Lauder
 - Computer Associates
 - Visa
 - British Telecom
 - Google
 - TJX
 - Brunswick
- The Center for Information Policy Leadership at Hunton & Williams

The Business Reality

- To succeed, every company must:
 - » Outperform the market
 - » Manage risks
 - » Deliver value to all its stakeholders
- Information fuels economic growth
- The ability to process information effectively and efficiently is the secret to success

Four Privacy Risks

- Legal compliance
- Reputation
- Investment
- Reticence

To be successful, you need to manage all of them.

U.S. Privacy Laws

- Major federal laws are:
 - » GLB: Financial institutions
 - » HIPAA: Health care entities
 - » FCRA/FACTA: Consumer reporting agencies
 - FTC Disposal Rule
 - » DPPA: DMV records
 - » CAN-SPAM: Commercial e-mail
 - » COPPA: Children's data
 - » Do-Not-Call Registry: Telemarketing
 - » FTC Act Section 5: Prohibits unfair or deceptive trade practices
 - » Privacy Act of 1974

State Laws

- California's AB 1950 and progeny apply to non-GLB, non-HIPAA covered entities
- Any business that owns/licenses PI must implement reasonable security procedures to protect the data from unauthorized access, destruction, use, modification or disclosure
- If the business discloses PI to a third party, there must be a contract in place to require the third party to maintain reasonable security procedures

U.S. Information Security

- 2005 was the year of the security breach
- In 2005/2006/2007, 430 information security breaches so far
 - » ChoicePoint - DSW
 - » Bank of America - CardSystems
 - » Lexis Nexis - Boston Globe
- Over 100 million potentially affected
- 30 plus state security breach notification laws
 - » California started the trend
 - » Service providers must report breaches to data owner so data owner can notify affected individuals

U.S. Privacy Laws and Outsourcing

- Privacy laws in the U.S. specifically contemplate the use of vendors
- But U.S. privacy laws don't yet address vendor relationships based on geography
 - » Proposed U.S. outsourcing laws
- Companies always remain accountable for actions by their agents
 - » And now we need to publicly announce vendor breaches!

The Bottom Line

- U.S. laws are not concerned with where personal information is processed – they are concerned with the safeguards that are in place to protect the data, wherever it resides
 - » Duties of vendor selection and oversight are the same, whether the vendor is domestic or foreign
- In considering any vendor relationship, security is a bigger concern than privacy
- Your focus should be on vendor management

Start with Due Diligence

- Know your vendor – establish a formal vendor qualification program
 - » Ability to meet your servicing, operational, financial and legal needs (given a possible foreign legal environment)?
 - » Established security program?
 - » Employee training?
 - » Ability to segregate your data?
 - » Ability to meet your standards?
 - » Audited when and by whom?
 - » Reputation for handling data carefully?
- Consider the parties' respective responsibilities in the event of regulatory changes in the U.S. or foreign country that could hinder the ability of the service provider to fulfill the contract

Understand the Deal

- What functions are being outsourced? What data is involved?
- Where will the data be going? Will it physically be transported there? Will remote access enable offshore workers to perform tasks? What level of access is needed?
- How do the vendor's security protocols match up with your own?

Build Standards into the Contract

- Standard confidentiality provision is a good start . . .
 - » Prohibit use/disclosure for any purpose other than to carry out the contracted services
 - » Service provider must implement a written information security program to safeguard data
 - » All data shared with service provider belongs to the company
 - » Indemnity (from service provider and any subcontractors)
 - » Audit right
 - » Termination clause

Build Standards into the Contract

- Add specific standards appropriate to the relationship
 - » Employee screening, monitoring, training
 - » Data transmission standards
 - » Access controls
 - » Audit trails
 - » Computer security standards
 - » Virus protection
 - » Incident response and reporting
 - » Insurance
 - » Remedies

Offshoring

- Consider how non-U.S. privacy laws interact with U.S. laws and how to manage conflicts
- May be exposed to country risk, i.e., economic, social and political conditions and events in foreign country may prevent service provider from carrying out the terms of agreement
- Closely monitor foreign government policies and politics in countries where service providers are located
- Establish procedures for dealing with country risk issues

Imagine the Worst Case Scenario

- Develop a formal response plan for a data security breach
- Don't rely on U.S.-based remedies
- What rights do you have under local law to recover data, prevent misuse?
- Identify local legal resources and map possible courses of action

Proactively Monitor

- Conduct periodic assessments
- Ask IT for its impressions, and follow up on concerns
- Adequate physical and data security controls? Contingency arrangements? Insurance coverage? Compliance with applicable laws and industry guidelines?
- Evaluate standards as the relationship evolves and new/different services are added
- Evaluate independent audit reports (internal and external)
- Monitor developing legal standards
- Monitor the vendor's financial condition as well

Outsourcing Requires Thought

- Survey says 25% would abandon a company that suffered a data breach
- Choose vendors carefully
- Determine whether applicable foreign laws are less protective of data and, if so, mitigate risk by contractually subjecting the overseas vendor to standards required by U.S. law
- Plan for incidents
- Consider exit strategy if the balance of risks shifts

Questions?

- Lisa J. Sotto
Partner
Head, Privacy and Information Management Practice
Hunton & Williams LLP
(212) 309-1223
lsotto@hunton.com

