

# Protecting Personal Information: Best Practices for Business

## Agenda

April 29, 2009

### 8:30 – 9:30 Registration

### 9:30 – 9:45 Opening Remarks

#### *Welcome and Introduction of co-sponsors*

**William Michael Treanor**, Fordham Law School Dean

**Leonard Gordon**, Regional Director, Northeast Region, Federal Trade Commission (FTC)

**Mindy A. Bockstein**, Chairperson and Executive Director,  
New York State Consumer Protection Board (NYCPB)

**Jonathan Mintz**, Commissioner, New York City Department of  
Consumer Affairs

### 9:45 – 10:25 Presentation — Risks & Costs: What's at Stake?

#### *Business and legal reasons to address data security including:*

- Federal laws and standards enforced, recent cases, and the costs, penalties, and relief imposed
- New York laws and standards enforced, recent cases and the costs, penalties, and relief imposed
- Prospects of private litigation against companies that experience a breach
- Other costs of data breaches — breach response costs, reputational damage, customer relations impact
- Other business rationales for improved data security

#### *Presenters:*

**Deborah Marrone**, Assistant Regional Director, Northeast Region, FTC

**Lisa R. Harris-Eglin**, Deputy Executive Director and General Counsel,  
NYCPB

### 10:25 – 10:30 Break

### 10:30 – 11:40 Panel 1 — Protecting Personal Information: Steps & Strategies

#### *Practical guidance and lessons learned from persons engaged in security compliance, addressing basic questions, such as:*

- What challenges have you faced in taking and maintaining an inventory of your personal information and equipment?
- How have you gone about determining whether you had adequate network and physical security?





- What data security challenges have you faced in hiring service providers and technical staff?
- How have you worked with outside IT professionals to address security issues posed by electronic information you use, maintain, store, or share?
- What issues have you confronted in determining what information to retain and what information to dispose of?
- What obstacles did you confront in persuading your organization to invest in better information security? How did you get top management involved?
- How did you balance the costs and benefits of compliance? How did resource availability affect your data security planning?

**Moderator:** Burke Kappler, Attorney, Division of Privacy and Identity Protection, FTC

**Panelists:**

**Deborah Joslyn**, Senior Manager, Privacy Team, Ernst & Young, LLP

**Scott Lancaster**, Director Information Security Group, Starwood Hotels & Resorts Worldwide, Inc.

**JoAnn Stonier**, Global Privacy and Data Usage Officer, MasterCard Worldwide

**Miriam Wugmeister**, Morrison & Foerster

## 11:40 – 11:50 Break

## 11:50 – 1:00 Panel 2 — When Things Go Wrong: Planning for & Responding to Data Breaches

***Breach response and the importance of planning ahead, including:***

- Anticipating and planning for a breach
- Responding when a breach occurs
- Breach investigation and maintenance of evidence
- Data and systems recovery
- Working with outsiders — what do law enforcement or technical professionals do when called in to respond to a breach, and what information do they look for and need?
- Notice and assistance to victims and consumers — how do consumers respond when a trusted business suffers a breach, and what is the best way for businesses to notify and communicate with customers in order to protect the relationship?

**Moderator:** Christopher Olsen, Attorney, Division of Privacy and Identity Protection, FTC

**Panelists:**

**James Jaeger**, Director, Cyber Defense and Forensics, General Dynamics

**Robert Novy**, United States Secret Service, Electronic Crimes Task Force

**Joel Reidenberg**, Associate Chief Academic Officer and Associate Vice President for Academic Affairs, Fordham University

**Lisa Sotto**, Hunton & Williams, LLP

## 1:00 - 2:00 Lunch