

# Protecting Personal Information: Best Practices for Business

## Agenda

April 15, 2008

Thorne Auditorium  
Arthur Rubloff Building

Chicago Campus  
Northwestern University  
School of Law

375 E. Chicago Avenue  
Chicago, IL 60611



**8:00 - 9:00 Registration**

**9:00 - 9:15 Opening Remarks**

- Welcome and introduction of co-sponsors

**9:15 - 10:30 Panel 1 – Risks & Costs: What’s at Stake?**

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

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

*Moderator:* Michael Atleson, Attorney, Federal Trade Commission

*Panelists:*

**Ruth Hill Bro**, Partner, Baker & McKenzie LLP

**Sgt. John Lucki**, Financial Crimes Unit, Chicago Police Department

**Christine Nielsen**, Assistant Attorney General, Consumer Fraud  
Division, Illinois Office of the Attorney General

**Larry Ponemon**, Ponemon Institute LLC

**10:30 - 10:45 Break**

**10:45 - 12:30 Panel 2 – How to Build a Culture of Security**

*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:** Laura Berger, Attorney, Federal Trade Commission

**Panelists:**

**Carol DiBattiste**, General Counsel and Chief Privacy Officer, ChoicePoint

**Justine Gottshall**, Partner, Wildman Harrold

**John Jensen**, Assistant Director, University Privacy and Security Office,  
University of Minnesota

**Vikki Kolbe**, Senior Vice President, Development and Delivery, HighRoads

**Judy Macior**, Vice President, Compliance and Information Practices, Experian

## 12:30 - 1:45 Lunch Break

*Attendees will be responsible for their own lunch.*

## 1:45 - 3:15 Panel 3 – 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:** Burke Kappler, Attorney, Federal Trade Commission

**Panelists:**

**Russell Collett**, Assistant Special Agent in Charge, United States Secret Service,  
Chicago Office

**Paul Luehr**, Managing Director and Deputy General Counsel, Stroz Friedberg LLC

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

**Amy Yates**, Director, Privacy and Data Protection, Deloitte & Touche LLP

## 3:15 - 3:30 Closing Remarks