

## **Compliance Management and Privacy Subcommittee Joint Session on Internal Compliance Measures for Data Security**

The Compliance Management and Privacy Subcommittees sponsored a joint session on internal compliance measures for data security at the Winter Meeting. Agnes Bundy Scanlan of Goodwin Procter LLP, Chair of the Compliance Management Subcommittee, moderated the panel; and the panel included Joanne Sundheim of JP Morgan Chase & Co. (Vice-Chair, Compliance Management Subcommittee), Patricia Covington of Hudson Cook LLP (Vice-Chair, Privacy Subcommittee), Amy Friend of the Office of the Comptroller of the Currency (OCC), Christine Frye of Countrywide, and Joel Winston of the Federal Trade Commission (FTC).

The session commenced with Agnes Bundy Scanlan's overview of data security breach issues, which included the following information regarding data breach incidents:

### **2005 U.S. Data Breach Incidents**

*166 disclosed incidents, potentially affecting more than 60 million individuals*

#### **Approximate breakdown by incident:**

Educational institutions -- 49%  
Banking/Credit/Financial institutions -- 14%  
Government/Military agencies -- 13%  
Retail companies -- 7%  
Health Care institutions -- 8%  
Data/Information companies -- 2%  
Other companies -- 7%

#### **Approximate breakdown by number affected:**

Educational institutions – 3%  
Banking/Credit/Financial institutions – 81%  
Government/Military agencies – 7%  
Retail companies – 3%  
Health Care institutions – 3%  
Data/Information companies – 1%  
Other companies – 2%

#### **Approximate breakdown by type of breach:**

Hackers or unauthorized access – 51%  
Theft of equipment – 29%  
Inadvertent disclosures – 20%

[\*\[Click here for additional documents that Ms. Bundy Scanlan provided to the participants.\]\*](#) .

Patty Covington provided the legal context for the discussion and discussed the differing components of states' data security breach legislation, [\*which is outlined on the attached chart.\*](#) For instance, the definition of personal information varied in Arkansas and Delaware (medical information included), North Dakota (mother's maiden name and employee identification

number included) and Georgia (pin password included). Minnesota had an exemption for financial institutions. North Carolina extended its legislation to include the media and all data including physical data. New Jersey has the strongest security breach law. In Illinois, Connecticut and Pennsylvania it is an unfair and deceptive practice to not provide notice to customers when their personal information has been breached. Twelve states have credit freezes. Patty noted that in 2006 seven additional states and jurisdictions are contemplating similar legislation: Arizona, Hawaii, Maryland, Michigan, Oklahoma, Wisconsin, and DC. There are twelve to thirteen federal bills being deliberated in six to eight Committees.

Joanne Sundheim and Christine Frye of JPMorgan Chase and Countrywide, respectively, spoke about data security best practices at their institutions. Joanne said that JPMorgan Chase assembled a corporate team and a team for each major line of business, each comprised of individuals with specialized expertise to manage response to a data breach. Their task is to minimize the harm to the customer, focus on the customers' trust, contain the issue, and limit exposure. This team employs internal controls to stop further breach and is responsible for the communications to internal employees, regulators and law enforcement. JPMorgan Chase's contracts with third parties have provisions regarding reporting an actual or potential breach.

Christine Frye spoke about Countrywide's practices. [Please see the attached documents that Christine provided to the participants.](#) Countrywide also has taken a corporate level approach to data security. There is a single point of contact for reporting a breach via e-mail, a toll free telephone number, etc. Countrywide has multiple regulators and has met with these regulators to establish common criteria and methods for notifying them of investigations. Countrywide's management receives weekly reports of all data security activity including investigations, consumer notifications, etc. Customer notification envelopes include a stamp on the cover entitled, "URGENT SECURITY INFO".

Amy Friend, OCC, and Joel Winston, FTC, spoke about the guidance and issues that have arisen under the guidance since March 2005. Amy responded to questions from bankers and shared the types of breaches the OCC has seen.

Many bankers asked the OCC if they had to report every breach. There is not a *de minimis* requirement and the OCC's response has been that bankers should have a discussion with their regulator. The reporting could range from incident to incident to reporting on a monthly basis, and again, this is a good opportunity for the banker to have dialog with their regulator. Bankers asked the OCC when they should notify customers. The OCC expects the bank to conduct an investigation to determine what the reasonable expectation is that customers' nonpublic information has been compromised or misused.

Joel Winston spoke about the existing laws relating to data security. He mentioned FCRA where the CRA can only provide consumer reports to those with a permissible purpose and must have reasonable "know your customer" procedures; FACTA where the disposal rule governs the proper disposal of consumer report information; GLBA safeguard rules; and the FTC Act's prohibition on unfair or deceptive practices. Mr. Winston also spoke about several FTC data security lawsuits regarding deceptive representations or unfair failure to have reasonable safeguard procedures.