



Panel: Data Privacy - Is Your Company Prepared?

Moderator: Jennifer Dioguardi
Snell & Wilmer (Phoenix, AZ)

jdioguardi@swlaw.com | 602.382.6371
http://www.swlaw.com/attorneys/jennifer_dioguardi

Don't Wait for a Data Compromise: Strategies for Prevention and Protection

Jennifer Dioguardi

Partner
Snell & Wilmer

Sherrie L. Farrell

Member
Dykema

J. Marcus Meeks

Associate General Counsel
Fannie Mae

Joseph J. Ortego

Partner
Nixon Peabody

Thomas E. Propson

Major Case Specialist, Business Tort Claims
Travelers Insurance

Don't Wait for a Data Compromise

- Data Breach:
 - Not a Matter of “IF”
 - Matter of “WHEN”

2

Privacy and Data Security at the Corporate Forefront

- The top concern for directors and general counsel
- Legal requirements have significant impact on businesses
- Data breach incidents are on the rise
- Data breach is a costly event for many reasons

3

Don't Wait for a Data Compromise

- Almost impossible to be in any type of business and not collect or hold Personally Identifiable Information (“PII”)
- PII includes but is not limited to:
 - Name
 - Address
 - Social Security Number
 - Date of Birth
 - Account Numbers (credit card, checking account)
 - Email Address
 - Passcodes

4

Don't Wait for a Data Compromise

PII could belong to:

- Employees
- Applicants
- Business partners
- Students
- Patients

5

Don't Wait for a Data Compromise

- Privacy can be of interest anywhere in the organization where personal information is processed.
- Although there are common processes in many organizations, there will also be industry-specific processes to consider.

6

Don't Wait for a Data Compromise

Common Processes:

- ❖ Human resource management
- ❖ Finance and accounting
- ❖ Procurement
- ❖ Marketing
- ❖ Sales
- ❖ Customer support
- ❖ Technical support
- ❖ Retail operations
- ❖ Research and development
- ❖ Regulatory reporting
- ❖ Vendor Agreements

7

Top Methods Used to Breach Data - 2012

- Theft – 32%
- Hacking – 21%
- Public Access/Distribution – 19%
- Unauthorized Access/Use – 10%
- Loss – 9%
- Virus – 4%
- Improper Disposal – 4%
- Unknown – 1%

8

Data Breach Notification Laws

- Legal notification requirements are complex
- State notification laws – state of residence of data breach victims
- Who must comply?

9

Shifting Risks on the Litigation Landscape

- Plaintiffs' "throw everything at the wall to see what sticks" strategy
- Measuring the effect of NIST framework in courts
- The shield of privilege



14

Activate Internal Response Team

- ✓ Emergency Contact Lists
- ✓ Executive Management Team
- ✓ Incident Lead
- ✓ Communications/PR
- ✓ Legal, Privacy and Compliance
- ✓ Operations (Security and IT)
- ✓ Customer Service and HR

15

Activate External Response Team

- ✓ Legal
- ✓ Forensic Investigator
- ✓ Mail-house for notification letters
- ✓ Call Center
- ✓ Consumer fraud protection
- ✓ PR

16

Identifying the Breach

- ✓ Consult legal counsel
- ✓ Internal IT Staff vs. Certified Data Forensics Agency
- ✓ Volume of records
- ✓ Nature of the specific information
- ✓ Cause
- ✓ Prevention

17

Evidence Collection

- ✓ Treat the incident as if it will lead to litigation or regulatory inquiry
- ✓ Keep evidentiary chain intact for electronic and physical evidence
- ✓ Give original records to legal and maintain a copy
- ✓ Keep records of all access to equipment and records
- ✓ Create itemized inventory of all evidence
- ✓ Executive-Level Report
- ✓ Technical Report

18

Pre-Notification Groundwork

- Customer confidence – minimizing customer churn
- Response mechanism in place prior to notification
- PR – message to the public
- Call Center scripts
- Website FAQ's

19

Notification

- **Content of Notice**
 - How the incident happened
 - What information taken
 - Company actions
 - Consumer protection solution
 - Contact information

20

Creating a Culture of Protecting Personal Information

- **Fannie Mae houses a large volume of Personal Identifying Information related to borrowers**
- **Various business units obtain and manage this personal data**
 - Loan eligibility
 - Loan servicing
 - Underwriting reviews
 - REO transactions
- **We've strived to create a culture where all Fannie Mae employees protect personal information**

21

Creating a Culture of Protecting Personal Information

- **Keys elements**

- Annual Training: Mandatory training once a year for all employees and contractors on privacy awareness, protection and reporting
- Targeted training
 - Training offered to key offices
 - Phishing tests
- Build a vernacular: Personal Information (PI) and Non-Public Personal Information (NPI) are defined in our relevant policies, stressed in trainings and used throughout the company as terms of art
 - "Is NPI involved?"

22

Creating a Culture of Protecting Personal Information

- Multiple reporting tools
 - A privacy mailbox
 - General ethics mailbox
- No Silos – all stakeholders engaged as part of normal business operations
 - Privacy Office
 - Operational Risk Management Office
 - Information Security Office
 - Technology Office
 - Internal Investigations
 - Legal

23

Creating a Culture of Protecting Personal Information

- **Tracking indicates a high level of employee awareness about privacy and available tools**
 - Privacy mailbox receives messages on a daily basis
 - High levels of self-reporting
 - 2013 ethics survey – greater than 90% of employees are aware of avenues for seeking advice on ethical issues and anonymous reporting
- **Anecdotal examples**

24

Data Breaches and Insurance Coverage

3rd Party Liability Coverage

- Commercial General Liability Policies
- Cyber Policies
 - Network Security Liability
 - Privacy Liability
 - Errors & Omissions Coverage

25

Data Breaches and Insurance Coverage

1st Party Coverages

- Crisis Management
- Identify Theft Response
- Cyber Extortion
- Network Business Interruption
- Contingent Network Business Interruption
- Data Asset Protection

26

Data Breaches and Insurance Coverage

Best Practices

27

About Jennifer Dioguardi
Partner | Snell & Wilmer | Phoenix, AZ

602.382.6371 | jdioguardi@swlaw.com
http://www.swlaw.com/attorneys/jennifer_dioguardi

Jennifer Dioguardi is based in Snell & Wilmer's Phoenix office where she serves as Co-Chair of the firm's Financial Services Litigation Group. Jennifer handles complex commercial litigation with an emphasis on banking, consumer financial services and securities litigation, FINRA arbitration proceedings, shareholder derivative litigation, D&O litigation, class actions, internal investigations and privacy and data security issues.

Jennifer's securities practice includes the representation of a number of financial institutions, including retail and investment banks, commercial lenders, underwriters, broker-dealers, investment advisors and publicly traded and privately held companies in federal court, state court and SRO arbitrations. She has represented these clients in matters involving claims for violations of federal and state registration and securities fraud statutes, directors' and officers' liability, shareholder derivative litigation, unsuitability, selling-away, churning, unauthorized trading and failure to supervise. Jennifer's practice also includes the representation of shareholders, officers, directors and corporations in connection with shareholder derivative litigation, D&O litigation and internal investigations.

Jennifer's financial services litigation practice includes the representation of national and local banks, merchant processing and service organizations, credit card issuers, mortgage lenders, automobile finance servicing organizations and securities broker-dealers in matters throughout the West. She has represented these clients in matters involving lender liability claims that include loan commitments, bad-faith dealing, termination of credit and wrongful acceleration of foreclosure, Truth in Lending Act (TILA), Fair Credit Reporting Act (FCRA), Real Estate Settlement Procedures Act (RESPA), Home Ownership Equity Protection Act (HOEPA), Electronic Fund Transfer Act (EFTA), Equal Credit Opportunity Act (ECOA), Community Reinvestment Act (CRA), Uniform Commercial Code (UCC), Unfair Debt Collection Practices Act (UDCPA), consumer fraud statutes, demand deposit account disputes involving check fraud, check kiting presentment and clearing issues, business torts and breach of contract issues. Jennifer has represented credit card issuers in disputes involving allegations of fraudulent transactions, authorized users, reversed charges, application of payments, interest rate disclosures and modifications, change in terms and fees and disclosures for related products and services. She has also represented merchant processors in litigation involving hold-backs, unauthorized business lines, termination, fees, commissions for merchant processor sales representatives and contract disputes involve merchant account agreements. Jennifer advises clients on privacy issues arising from the collection and use of consumer non-public personal financial information.

As a member of the Snell & Wilmer Hiring Committee, Jennifer is actively involved in bringing the brightest young lawyers to the firm.

Education

- University of Arizona (J.D., magna cum laude, 1997) -- Phi Delta Phi; Dean's List; Order of the Coif; Editor-in-Chief, Arizona Journal of International & Comparative Law
- University of Washington (B.A., 1991)