Navigating Regulatory Impacts of a Financial Services Data Breach

Stacey C. Bolton, CIPP
SVP, Global Head of Privacy and Information Management
The Northern Trust Company

Email: scb8@ntrs.com
Phone: 312-557-1558
2011 Incidents by Vector

Inside-Malicious - 11%
Unknown - 9%
Inside - 8%
Outside - 53%
Inside-Accidental - 19%

http://datalossdb.org/statistics
2011 Incidents

**Incidents by Data Type**
- Date of Birth - 9%
- Social Security Number - 10%
- Miscellaneous - 15%
- Names - 24%
- Medical - 8%
- Address - 8%

**Incidents by Business Type**
- Medical - 20%
- Government - 16%
- Educational - 11%
- Business - 53%
- Medical - 8%
- Government - 16%
- Educational - 11%
- Business - 53%
# Key US Privacy Laws and Regulations

## Gramm-Leach Bliley Act
- FIs must protect non-public personal info of consumers and customers
- Initial and annual privacy notices
- Consent requirements and Opt-out Notice
- Interagency Guidelines requires written Info Security Plan with appropriate incident response procedures

## Fair Credit Reporting Act
- Governs uses and disclosure of information in consumer reports by consumer reporting agencies
- Provides access rights to consumer
- Red Flag Rules requires creditors to develop identity theft prevention programs

## HIPAA/HITECH Act
- Governs use and disclosure of Protected Health Information (PHI)
- Individuals **have** right of access to inspect PHI
- HITECH amends HIPAA to include security breach notification requirements & expands applicability of HIPAA to business associates
- Employer-sponsored Health Plans must certify compliance with HIPAA Privacy Standards

## State Data Security Laws
- Massachusetts law requires covered entities to implement administrative, physical, and technical safeguards around PII.
- 46 states, DC, Puerto Rico & BVI have enacted notification laws involving security breaches of PII. (CA, IL, NY, ND, OK, SC, TN, TX, ME, MA, MN, NV – unauthorized acquisition)
# Key International Privacy Laws and Regulations

<table>
<thead>
<tr>
<th>EU Data Protection Directive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Includes European Union Member states: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, UK (also new member states)</td>
</tr>
<tr>
<td>• Six tenants: Notice, Choice, Use, Security, Correction &amp; Enforcement</td>
</tr>
<tr>
<td>• Includes natural person identified by an identification number or physical, physiological, mental, economic, cultural, or social identity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EU and US Safe Harbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To qualify for Safe Harbor, organization must: (1) adhere to the 7 guiding privacy principles, and (2) publicly announce its compliance through certification letters filed annually with the Dept. of Commerce</td>
</tr>
<tr>
<td>• Banks, investment houses, credit unions, savings &amp; loan institutions, non-profit organizations, insurance companies and meat processing facilities currently ineligible for Safe Harbor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Various Implementing EU Country Laws and Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Many member states have enacted laws implementing the EU Data Protection Directive (i.e. UK Data Protection Act 1998)</td>
</tr>
<tr>
<td>• New Proposed UK Privacy Law</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Country laws (e.g. Canada, Japan, Mexico)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Canada - PIPEDA governs the topic of data privacy, and how private-sector companies can collect, use and disclose personal information.</td>
</tr>
<tr>
<td>• Japan - Act aims to &quot;protect the rights and interests of individuals while taking consideration of the usefulness of personal information.&quot;</td>
</tr>
<tr>
<td>• Mexico - Federal law deals with data subjects' rights, security and breach notification provisions, cloud computing, consent and notice requirements, and data transfers.</td>
</tr>
</tbody>
</table>
Organizations often have a very robust level of security and communication around the protection of **personally identifiable information** (PII) to prevent it being shared, intentionally or unintentionally, with parties not authorized to view that data. Many organizations also have created controls around Confidential and/or Proprietary Information.

### What is personally identifiable information (PII)?

PII is information which can be used to determine the identity of any **individual**, or to permit access to or to create a new personal account, specifically: a person’s name, address, or telephone number, **in combination with**:

- Social Security number, Social Insurance number or any other tax identification number
- Drivers license number, Account number, credit card number or debit card number,
- or a personal identification number or password that would permit access to the customer’s account.

### Account access information:

Information which would permit access to any (personal or corporate/institutional) customer’s account, specifically an account number/username **in combination with** a PIN, password, passphrase or any other information that can be used to access a client’s account.

### What is Confidential and/or Proprietary Information?

Confidential and Proprietary Information generally means **non-public information where disclosure could result in serious damage to a company or a client**. Examples include but are not limited to:

- All information about company’s past, present and prospective clients and all information received from them, including the fact that an individual or entity is a customer.
- Competitive matters, such as confidential plans and activities, its technology and its trading positions.
- Nonpublic information that might affect the price of a public company’s stock, such as information about its current or projected earnings or a potential transaction, such as an acquisition.
- Nonpublic financial reports or projections.
Common Events

- Laptops or portable media devices (e.g. PDA, CD, flash drive etc.) are lost or stolen
- Client statements, confirmations, tax information, checks are sent to another client
- A hacker illegally gains access to systems and customer information
- Fax is sent to the wrong location
- A courier delivers a package to the wrong address
- System Access is granted to the wrong customer
The Biggest Culprit

Email Reminders You MUST Communicate to Employees

- Before forwarding or replying to an email, check the history of a message. Make sure that the content of the email is appropriate for the recipients.

- Delete or mask PII or Account Access Information when possible.

- Check the attachments for any sensitive or incorrect client data (check for hidden fields in Excel files).

- Do not email information to your personal address in order to "work from home" - use the institution’s approved remote access solutions.

- Double check the recipients of any message you send, especially when distribution lists or external email addresses.

- A pop-up message box will indicate when an email is going to a non-NT recipient. Read and follow the message carefully.
Example Pop-up Message

Internet Email Address Confirmation

This email contains an address outside of the Northern Trust network. By continuing you confirm the addressees are correct.

If this email contains Personally Identifiable Information concerning a client, prospect or partner, you must encrypt it in compliance with the Northern Trust Email Standard.

Failure to observe the Email Standard or causing a breach through misdirected email is subject to disciplinary action up to and including termination.

Please select 'YES' to continue sending or 'NO' to cancel and return back to the email.

Yes  No
Communicate clearly and often how employees are to notify the Privacy Office of any potential breach (loosely defined as any incident in which “sensitive” information has been sent or received by an unauthorized third party).

- Send an **e-mail to Privacy Office** or **call a Privacy Hotline**, with detailed information about the incident or potential breach so that the Security Breach Response Team (SBRT) can begin an investigation.
- Notify your manager
Role of the Privacy Office

Receive ➔ Assess ➔ Contain ➔ Escalate ➔ Notify ➔ Remediate ➔ Validate
KNOW Your Key Stakeholders

- Sr. Management or Business Unit Execs
- Counsel (in-house/external) Enforcement
- Insurance
- Technology
- Call Center
- Regulators/Law enforcement
- Public Relations
Privacy Office (PO) alerted of potential Breach and analyses if breach is reportable based on Breach Notification Laws.

If yes, PO follows Breach Notification Protocol (See Breach Notification Chart).

PO follows remediation protocol (See Remediation Protocol Chart).

If no, PO determines if non-reportable incident requires remediation.

If yes, PO follows remediation protocol (See Remediation Protocol Chart).

If no, PO logs incident and formally closes.
Privacy Breach Notification Protocol

1. Analyze both regulatory and contractual disclosure requirements
2. Provide notice to regulatory authorities (Federal, State, International)
3. Draft customer/consumer notifications in compliance with state, national and international regulations.
4. Consider staggered notification for large breaches, and make sure that PR is involved and call centers are briefed with approved responses.
Remediation Protocol

- **Root Cause Analysis**
  - Privacy Office commissions a detailed report from the business/department concerning the cause of the incident.

- **Control Assessment**
  - Privacy Office analyzes the cause to determine if the incident was the result of a control weakness.

- **Remediation Plan & Closure**
  - Privacy Office works with business/department to create a remediation plan that addresses future breach risk.
  - This action formally closes the incident.

- **Control Validation**
  - Periodically, business/department engages audit/testing function to validate effectiveness of mitigating controls.
Top Ten Privacy Threats

10-GEO Tags
9- Google Wi-Fi Sniffing
8-Facial Recognition Technology
7-Internet Censorship
6-Smartphones
5-Data-Stealing
4-Behavioral advertising
3-Hackers
2-Social networks
1-You!
## Loss Recovery – The Role of Insurance

<table>
<thead>
<tr>
<th>Coverage Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal and Defense Expenses</strong></td>
<td>Offers coverage for legal liability, defense costs and expense reimbursement for liability from a personal identity event.</td>
</tr>
<tr>
<td><strong>Notification Expense</strong></td>
<td>Coverage for the reasonable and necessary costs incurred for correspondence or other communication directed to individuals whose personal information is subject of personal identity event.</td>
</tr>
<tr>
<td><strong>Regulator Expenses</strong></td>
<td>Coverage for reasonable attorney’s fees and expenses for legal services incurred in the defense of regulatory action against the insured because of identity event.</td>
</tr>
<tr>
<td><strong>Crisis Management Response</strong></td>
<td>Coverage for charges and fees for the services of a public relations, crisis management or law firm to help restore confidence of the insured’s customers and investors.</td>
</tr>
<tr>
<td><strong>Identity Theft Recovery Expense</strong></td>
<td>Coverage for reasonable fees and expenses incurred by an insured for any service specifically approved, including identity theft education and assistance and credit file monitoring.</td>
</tr>
<tr>
<td><strong>Security Breach Insurance</strong></td>
<td>Third party liability coverage for claims resulting from a failure of computer security, including privacy claims.</td>
</tr>
<tr>
<td><strong>Business Interruption</strong></td>
<td>Protection for business interruption losses arising from the interruption or suspension of an insured’s computer network due to failure of network security.</td>
</tr>
<tr>
<td><strong>Cyber Extortion</strong></td>
<td>Coverage that provides protection for both first-party loss and third-party liability resulting from acts of cyber terrorism.</td>
</tr>
</tbody>
</table>