

**Managing a Data Breach:
A Five-Step, South Carolina Survival Guide
for Senior Managers,
In-House Counsel, Risk Managers
and Security Officers**

June 25, 2009

Jon Neiditz, jon.neiditz@nelsonmullins.com/404.322.6139

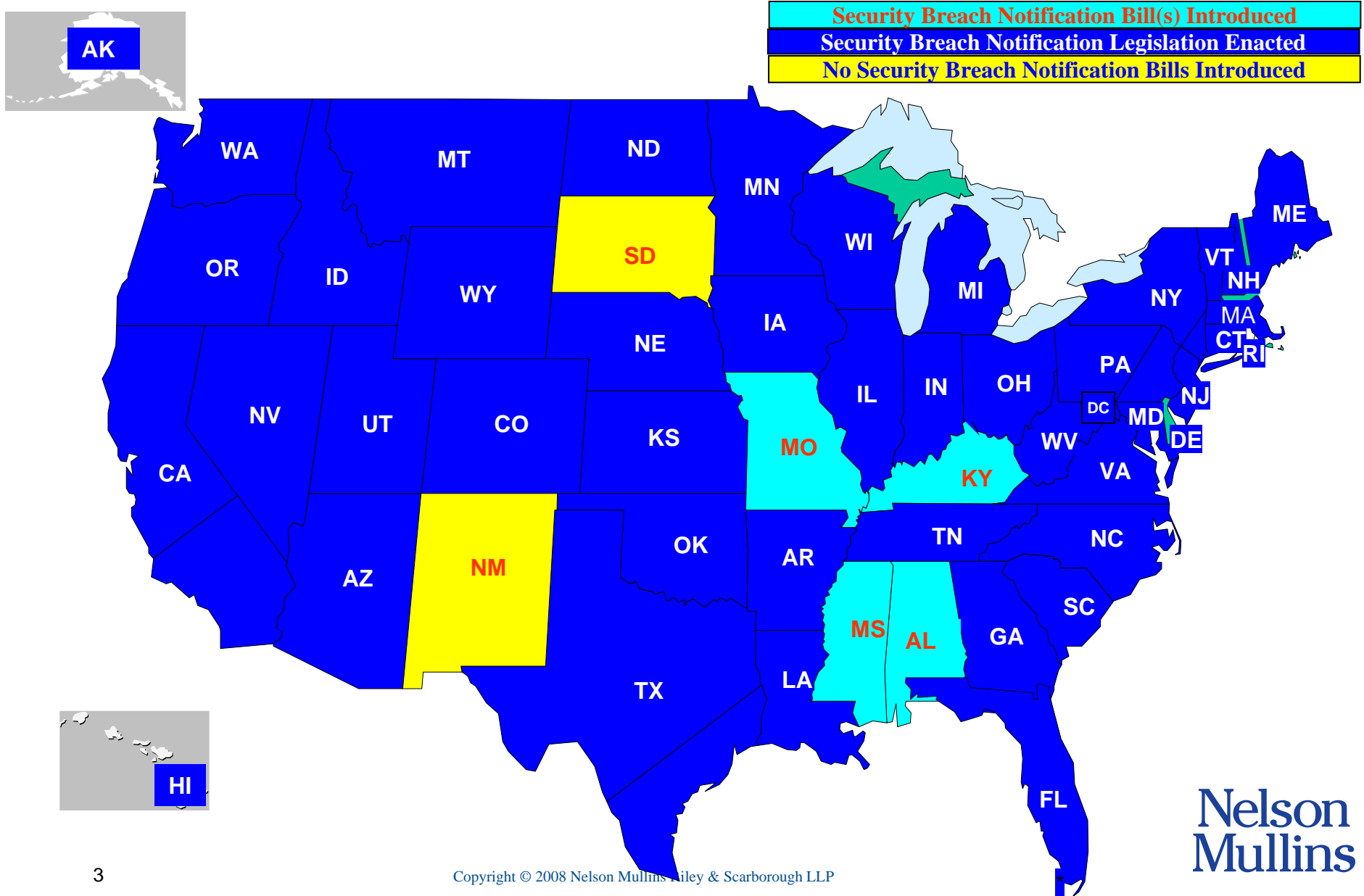
**Nelson
Mullins**

Introduction

**A Public-Private Patchwork, with Private Security Standards
Beginning to Dominate**

	Private Enforcement	Regulatory Enforcement	Enforcement Through Competition	Court Enforcement
Private Standards	e.g., Payment Card Industry Data Security Standard (PCI DSS), AICPA's GAPP, IIA's GTAG, ISO, ANSI	FTC enforcement of APEC Privacy Framework, HIPAA deference to WEDI, "deemers"	new privacy competition between ISPs, "best practices"	private and/or Government Standards become Liability standards
Government Standards	e.g., outsourcing and other vendor contracts (including HIPAA business associate contracts, GLBA service contractor agreements, EU contracts for data transfer)	e.g., GLBA enforcement by "functional regulators," FTC Act Section 5 authority, FCRA/FACTA	e.g., handling of breaches and provision of monitoring/insurance	e.g., e-discovery, attempts at security breach class actions

Introduction

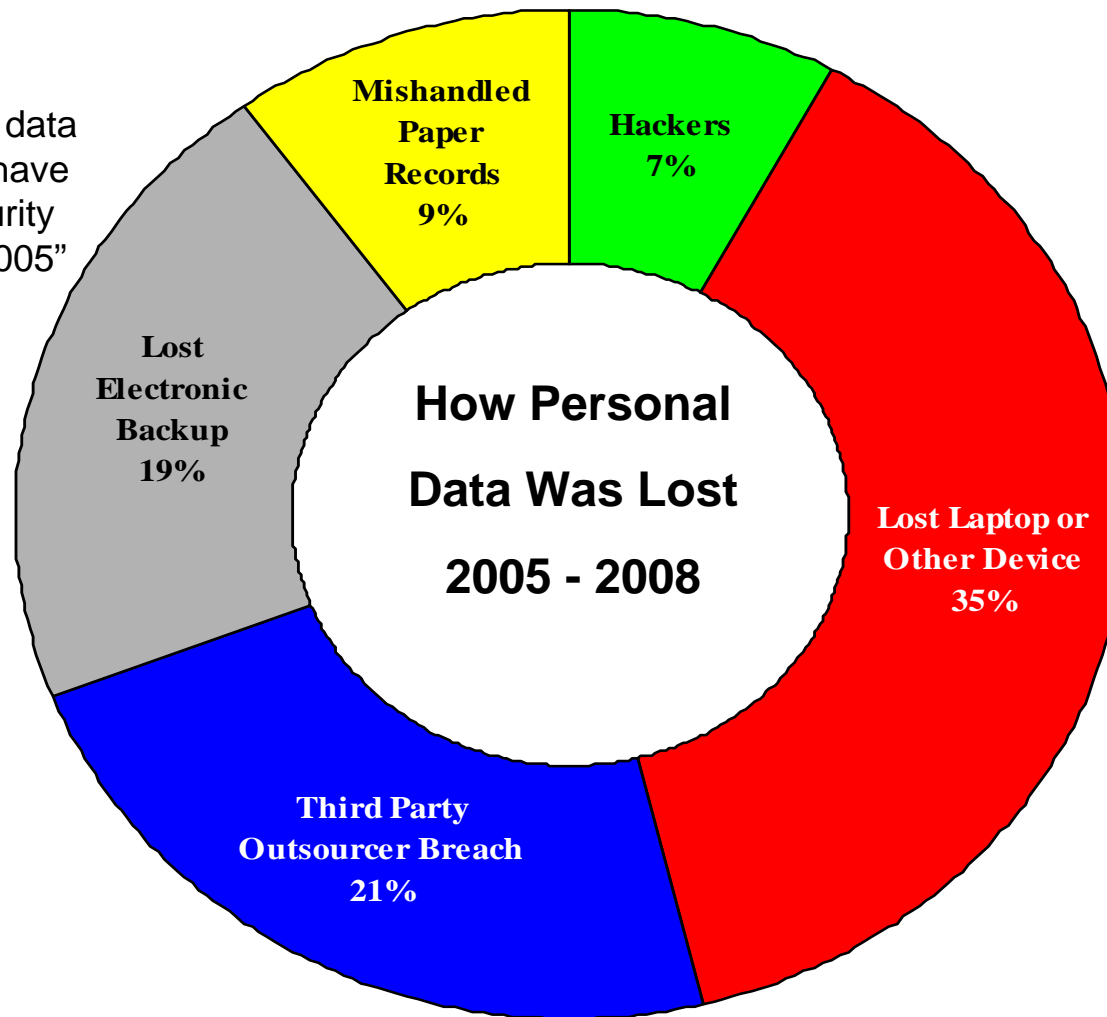


Introduction

Privacy Risk

“Over 236,805,918 million data records of U.S. residents have been exposed due to security breaches since January 2005”

- Source Privacyrights.org 8/08



Introduction

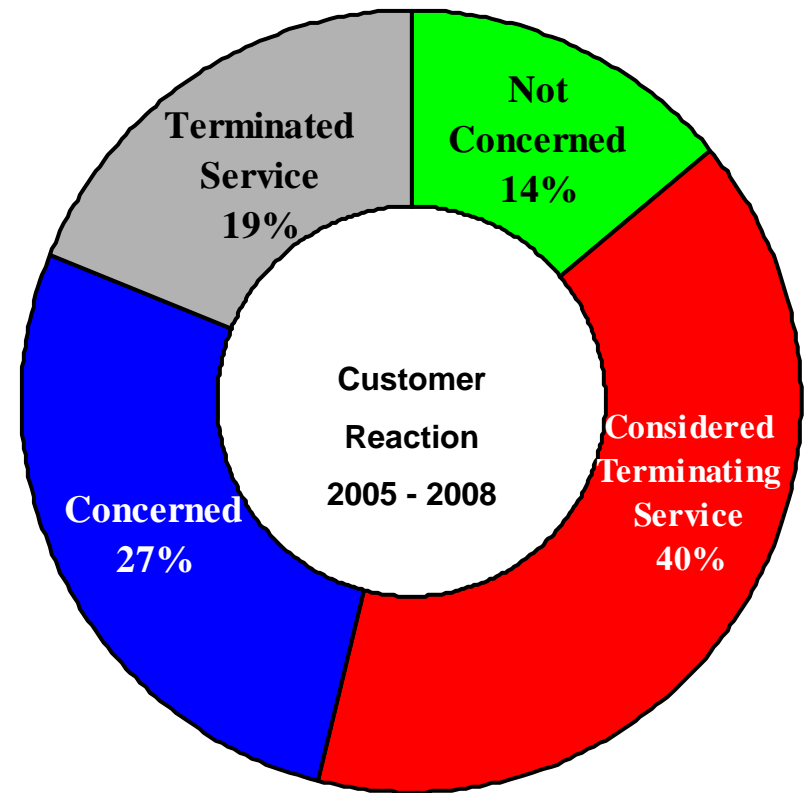
Cost of a Privacy Breach



\$182/customer

Source – Wired Magazine 2/07

Customer Reaction to A Privacy Breach



Average Cost Per Incident

\$6,300,000

Source: Ponemon Institute

**Nelson
Mullins**

Why Have A Breach Management Plan

- Consumer businesses **may lose 20% to 30% of their customers** that receive breach notices from them:
 - Only 8% of consumers who receive a security breach notification did not blame organization that sent the notice (usually the “owner or licensee”)
 - Over 40% said they might discontinue their relationship
 - Another 19% said that they had already done so

Source: Ponemon Institute Surveys, 2005 and 2008 (30% is 2008 number)

- Failure to handle the issue to customers’ satisfaction can result in further brand damages
- Failure to respond quickly can result in larger problems
- Having a clear response to the crisis can make a huge difference in response **time** and **cost**.
- In many cases, organizations can spend up to **\$92 per record** following a breach. A well managed breach can cost less than **\$30 per record** for an identical response with proper planning.

Extreme Costs and Variations in Cost (Aon Data)

Scenario 1 = Costs through Litigation

Scenario 2 = Pre-Litigation Costs

Scenario 1: Breach Management Plan: A financial services provider discovers a complex virus that had slowly transmitted out nearly **600,000 customer records** over a 2 year period. Once the company went public a class action lawsuit quickly follows alleging that customers were victims of ID Theft. The recently settled incident had the following costs.

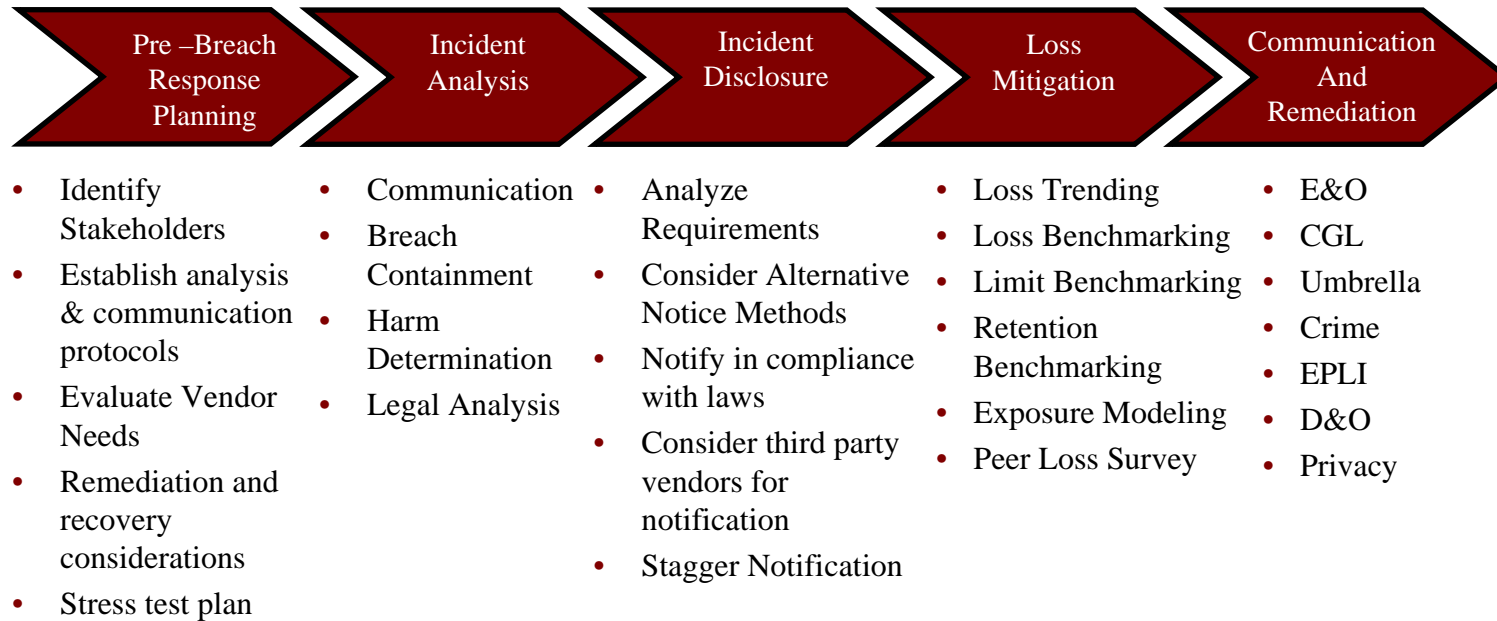
Scenario 2: No Breach Management Plan: A services provider to the entertainment industry suffers a virus attack that leaks data over a 3 year period resulting in over **500,000 lost customer and employee records**. A lawsuit is pending. The incurred losses to date

Expense Type	Cost
Technical Forensics	\$225,000
Legal Expense	\$15,000
ID Theft Forensics (initial and ongoing)	\$900,000
Mailing costs - 3 complete mailings Includes embedded legal costs as well as privacy and secondary notification to the "class"	\$1,600,000
Call Center (Overflow only. Mostly handled in house)	\$75,000
Public Relations Expense	\$50,000
Credit Monitoring (variable rate per activation: 10% - 15%)	\$1,900,000
Defense Costs	\$1,100,000
Additional Settlement Costs (including plaintiffs fees, and TPA ID theft claims)	\$3,000,000
Total	\$8,865,000

Expense Type	Cost
Technical Forensics	\$40,000
Legal Expense	\$5,000
ID Theft Forensics	\$0
Mailing costs 1 mailing	\$1,500,000
Call Center (Outsourced)	\$400,000
Public Relations Expense	\$20,000
Credit Monitoring (blanket purchase @ fixed rate)	\$7,500,000
Defense Costs	\$190,000
Additional Settlement Costs	\$0
Total	\$9,655,000

The Five Step Survival Guide

Security Breach Management Framework



The Five Step Survival Guide



Pre Beach Response Planning

- **Identify Stakeholders**
 - Business Unit Representatives
 - Privacy Officer / Legal / Compliance
 - Information Technology;
 - Risk Management;
 - Disaster Recovery / BCP
 - Public Relations
 - Vendor Management
- **Establish Analysis and Communication Protocols**
- **Evaluate Vendors Needs**
 - Technology – to handle technical forensics
 - Legal – to assist in determining notification obligations and drafting letters/call center script
 - Call Center – to handle inbound calls from victims
 - ID Theft Mitigation – including credit monitoring and other solutions
- **Remediation and Recovery Considerations**
 - Contractual Indemnities
 - Insurance Policies
- **Stress Test Plan Annually**
- **Ensure the Stakeholders have authority to act instantaneously**

The Five Step Survival Guide



Security Breach Incident Analysis – The Basics

- **Communication** - Ensure that decision makers receive real time information
- **Breach Containment** – Can breach be contained and stopped without destroying critical evidence? Should an internal or external firm be used?
- **Harm Determination** – Technical forensics are usually valuable and **almost always** necessary in connection with insurance coverage. Choose third party vendors carefully to minimize expense and avoid PCI issues. Consider specialized ID Theft Forensics as part of the strategy.
- **Legal** - Involve legal counsel immediately to avoid legal and regulatory pitfalls. **Strongly** consider involving outside counsel specializing in privacy and security laws.

The Five Step Survival Guide



Security Breach Incident Analysis – Important Questions in Dealing with Breaches

- Acquisition (or access) vs. harm
- All businesses vs. exclusions for privacy regulated entities or only “information brokers”
- Non-electronic data included?
- Personal information: The original California list vs. adding additional elements
- How soon notification must take place
- Report to authorities required?
- Law enforcement coordination exception?
- Pre-breach measures required?
- Civil/criminal penalties and/or private right of action

The Five Step Survival Guide



Security Breach Incident Analysis – South Carolina

- Notice is triggered only when illegal use has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident
- In addition to the usual elements of notice-triggering information (name + SSN, driver's license #, account number + PIN), includes:
 - other numbers or information which may be used to access a person's financial accounts or
 - numbers or information issued by a governmental or regulatory entity that will uniquely identify an individual
- GLBA exception (and exception for banks subject to Interagency Guidance)
- Pre-breach measures include rules on disclosure of SSNs and secure destruction requirement
- Notice must take place in the most expedient time and manner possible and without unreasonable delay
- Private right of action
- Must inform Consumer Protection Division of Dept. of Consumer Affairs & all national Consumer Reporting Agencies if notifying 1,000+ persons

The Five Step Survival Guide



Security Breach Incident Analysis – North Carolina

- Illegal use/harm threshold the same as SC
- Breach of **paper** documents clearly included
- In addition to usual elements of notice-triggering information includes:
 - checking or savings account #
 - credit or debit card #,
 - PIN,
 - digital signature,
 - biometric data,
 - fingerprint or
 - passwords
- Notice-triggering information also includes electronic ID #, email names or addresses, parent's maiden name or any other #s if they permit access to financial resources
- No GLBA exception for breach notification, but pre-breach measure requirement excludes entities covered by GLBA, FCRA and HIPAA
- Private right of action if injured
- Report to Consumer Protection Division of Attorney General's Office and Consumer Reporting Agencies if notifying 1,000+ persons



The Five Step Survival Guide



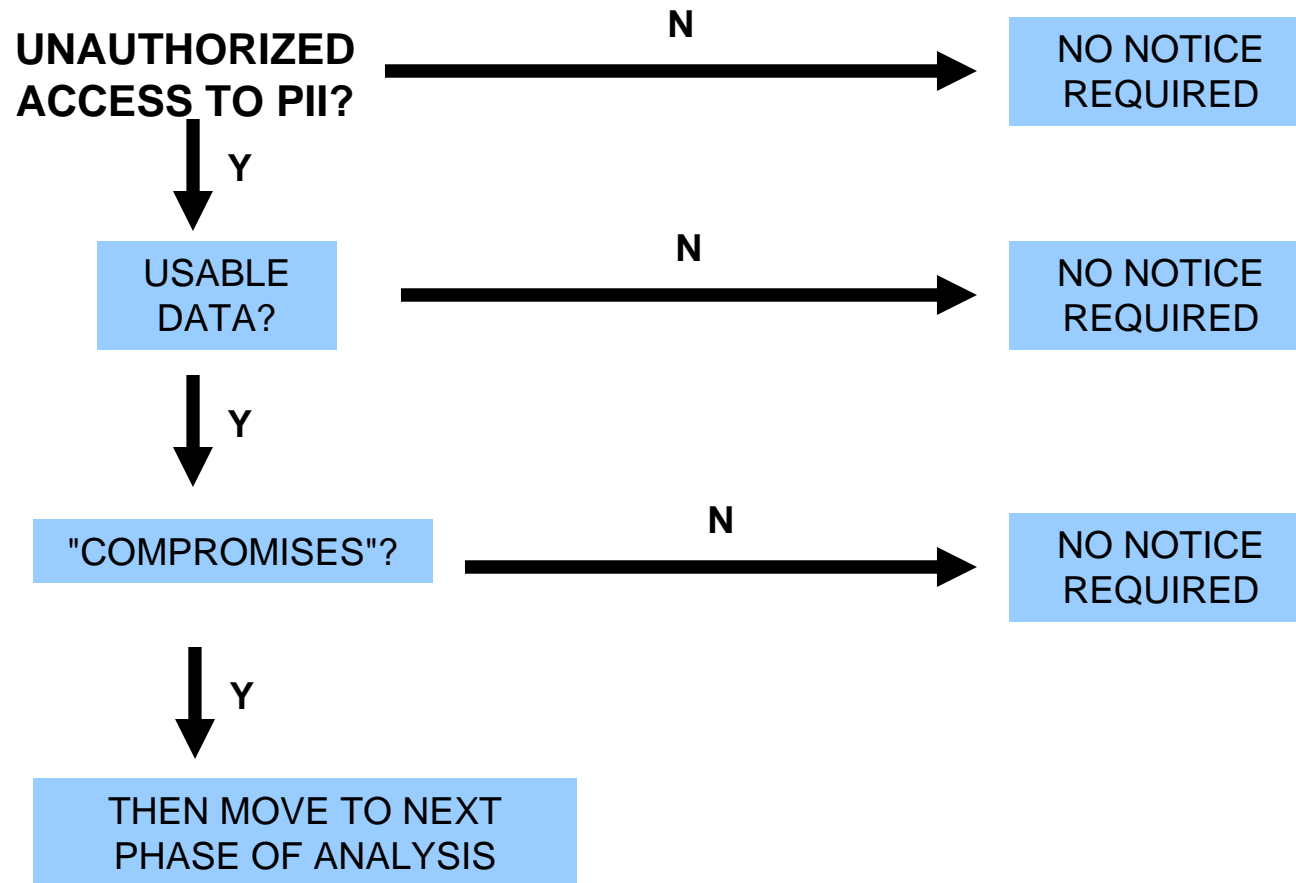
Security Breach Incident Analysis – Deeper Dive Into South Carolina

- Some portions effective December 31, 2008.
 - Use of SSNs
 - Requirements before disposal or transfer
- Breach notification portions effective July 1, 2009.
- **"PII"**
 - includes a person's first name/initial, last name, WITH
 - SSN, driver's license or ID card number;
 - Financial account number or card number and access code/password that would permit access to financial account; AND/OR
 - Other information allowing access to a person's financial resources or will uniquely ID a person.
 - does not include information lawfully obtained from public information or from government records lawfully made available to public

The Five Step Survival Guide



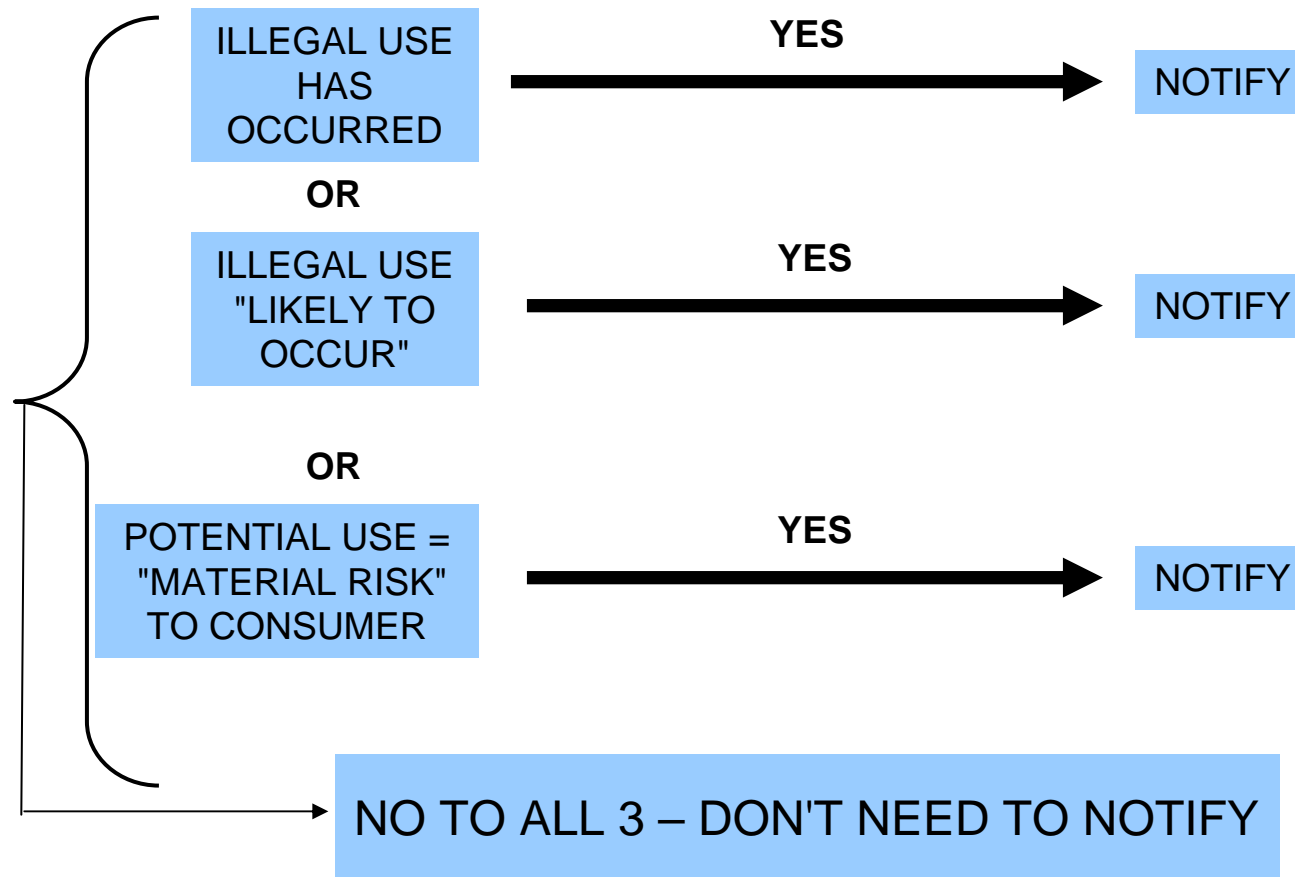
Security Breach Incident Analysis – South Carolina Decision Tree 1



The Five Step Survival Guide



Security Breach Incident Analysis – South Carolina Decision Tree 2



The Five Step Survival Guide



Security Breach Incident Analysis – Encryption Safe Harbors

- The security bar has been set by law ever-more-clearly at "encryption," vaguely defined (except in Wyoming)
- Massachusetts rules that continue to be put off contain significantly more detailed physical, administrative and technical security requirements than previous sets of legal requirements
- Like the breach notification laws and the Nevada law effective 10/1/2008 (and similar laws considered in Washington and Michigan), the Massachusetts rules push organizations more strenuously toward encryption than does older security regulation:
 - Organizations must, to the extent technically feasible, encrypt "all transmitted records and files containing personal information that will travel across public networks, and encrypt all data to be transmitted wirelessly."
- Note, however, that the stimulus package is a game-changer....

The Five Step Survival Guide



Security Breach Incident Analysis – The Immediate Future Under ARRA

- Breach notification obligations for not only HIPAA-covered entities but HIPAA business associates turning on "unsecured PHI"
 - The combinations triggering notice under all state laws (initially designed to address the major causes of identity theft) jettisoned
 - Paper and even oral breaches (apparently) included
 - Exceptions
 - 60-day outside limit for notifications, but should be more prompt in the absence of justification
 - DHHS must be notified for breaches involving more than 500 people
- Secretary of DHHS to issue annual guidance on technical safeguards
 - Does not yet appear to favor encryption over other safeguards, contrary to all state breach laws, MA and NV laws, and guidance for federal financial institutions
- Enforcement by state AGs, more stringent remedies and shift in burden of proof

The Five Step Survival Guide



Security Breach Incident Analysis – The Immediate Future: FTC Rules

- The FTC just proposed breach notification rules that apply to non-HIPAA covered entities and non-BAs that are vendors of personal health records, PHR related entities and their service providers (i.e., Google and Microsoft).
- Breach defined as acquisition of PHR identifiable health information **without the authorization of the individual** unless reliable evidence showing there has not or could not be unauthorized acquisition.
- Under the proposed rules, an entity that has suffered a security breach must notify all US citizens (presumably international notification is required) and US residents **without unreasonable delay**, but **no later than 60 calendar days** of discovery unless law enforcement requires a delay.
- Must also notify the FTC after a breach. If the breach impacted 500 or more, must notify FTC **within 5 days** of discovery of breach. If less than 500, must keep breach log and submit it annually to the FTC.
- Applies to breaches that are discovered on or after **September 18, 2009**.
- HHS breach rules still to follow.

The Five Step Survival Guide



Security Breach Incident Analysis – The Immediate Future: HHS Guidance

- On April 17, 2009, HHS issued proposed guidance identifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, as required by the Health Information Technology for Economic and Clinical Health ("HITECH") Act passed as part of ARRA.
- Only 2 approved methods: **encrypt** or **destroy**.
- Generally, for electronic PHI to be encrypted it must be encrypted using “an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and such confidential process or key that might permit decryption has not been breached.
- 2 types of **encryption** specified: for data at rest (with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices) and for data in transit (those that comply with the requirements of Federal Information Processing Standards ("FIPS") 140-2).
- 2 methods of **destruction** specified: for non-electronic media (paper, film, or other hard copy media should be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed) and for electronic (electronic media should be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved).

The Five Step Survival Guide



Security Breach Incident Analysis – Other Considerations

- **Many** forensics firms, PR firms and credit bureaus offer products that bundle breach-related services
 - Be very careful about listening to any vendor that has a financial interest in notification or other services
 - Make sure you get a quick, independent, expert read on legal requirements and whether and how notice should be given
- In-depth technical forensics often are valuable where they are not intuitively needed. Don't make assumptions!
- The great majority of breaches are not notice-triggering and may be addressed very quickly and inexpensively. Involve legal counsel early in the process.
- When breaches are notice-triggering, the quality of the communication matters.

The Five Step Survival Guide



Security Breach Incident Disclosure – Core Considerations

- Analyze disclosure requirements including regulatory requirements and contractual obligations. Don't overlook encryption safe harbors
- Notify compliance with state, national and international regulations. *Consider taking advantage of alternative notification techniques.*
- Consider a blanket notification to everyone impacted by the breach. It's very expensive and in most cases, it's unlikely that insurance will consider notification that is not required by law;
- The quality of the communication matters. Instructional papers have been written about the do's and don'ts of disclosure letters.
- Many firms offer notification services at costs less than 1.50 per record. Sample services available include:
 - Address procurement;
 - Mail merges;
 - Printing, sorting and mailing;
 - Secondary notification where addresses have changed and letters “bounce”
- Consider staggered notification for large breaches
- Make sure that Public Relations is involved and employees are briefed on responding to clients. **Make sure a unified message is sent.**

The Five Step Survival Guide



Security Breach Loss Mitigation – Loss Mitigation Solutions

- Coupons, Cash and Other Options – Some organizations utilize coupons, cash or credits as a loss mitigation solution. The initial statistics show this method is fairly effective.
- Credit Monitoring – TransUnion, Equifax and Experian offer credit file monitoring solutions with daily alerts of any inquiries or changes to credit files. They usually also offer access to credit reports
- ID Theft Analytics – Some organizations, such as ID Analytics specialize in monitoring customer databases for instances actual identity theft. In some cases, they have been able to significantly reduce overall costs associated with breaches.
- Fraud Monitoring / Credit Freeze – Some firms offer fraud monitoring and will even freeze your credit files forcing credit providers to contact you directly in the event someone applies for credit in your name
- Identity Theft Resolution – There are numerous services that offer 1-800 access to full time credit counselors and fraud resolution specialists.
- Identity Theft Expense Reimbursement Insurance – Reimburses victims for up to \$2,000,000 per person for costs in managing identity theft. Coverage is fairly narrow.
- Package Solutions – There are package solutions available that include credit monitoring and fraud monitoring for credit files, public records, applications and healthcare records. Please follow the link below for details: http://www.nextadvisor.com/identity_theft_protection_services/compare.php?kw=gidxx2%20identity%20theft%20protection
- Solutions for children are problematic.
- International solutions are a big problem.
- There are dozens of solutions available, but only a few that offer anything of value.

The Five Step Survival Guide



Credit Monitoring Package Basics

- Credit File Monitoring – 12-36 months of single or tri-bureau credit monitoring of victims credit files with daily alerts of any inquiries or changes to credit files
- Identity Theft Assistance – Most Credit Monitoring Solutions include access to 1-800 access to full time credit counselors and fraud resolution specialists.
- Identity Theft “Insurance” – Reimburses victims for up to \$25,000 per person for costs in managing identity theft.
- Credit Reports - Access to credit reports for 30 days to 12 months
- Extras – Including access to identity theft publications, credit scoring and credit simulators

Credit Monitoring Purchasing Concerns

- Options & Length– Single bureau and multi bureau packages are available. Most organizations opt for 6-12 month solutions, but some companies are considering multi-year packages
- Jurisdictional Concerns – Most credit monitoring packages are limited to US residents. Further, the ID Theft “Insurance is not available in all jurisdictions.
- Signup - Signup process for victims is typically web only. Signup by mail and/or phone can generate an additional fee.
- Call Centers – Many CRA Solutions include 1-800 access to credit/fraud resolution specialists. The “hand off” between the notification call center and the CRA call center can be a major problem.

The Five Step Survival Guide



Additional Credit Monitoring Purchasing Concerns

- **Contracting**– Some CRA’s attempt to limit their liability to the costs of fees charged. The contracts are complex and many legal departments take weeks negotiating.
- **International Considerations** - For the most part, credit monitoring is available in a handful of countries. International breach solutions will need to be pieced together using a myriad of vendors around the world. If possible, use a firm that has the best international capabilities.
- **Multilingual Issues** – Some CRA’s offer portions of their service in English only.
- **Scalability** – Not all firms that offer credit monitoring solutions have the ability to scale their services to more than 100,000 records.
- **Minimum Fees** – In some cases, CRA’s have set up fees of 40k-100k and others are willing to negotiate turn-key purchase orders with no expiration that only bill once the first customer
- **Billing** – Many companies fall into the blanket purchasing trap. The best way to reduce costs is to consider purchasing a solution on a per activation basis.

The Five Step Survival Guide



Communication & Remediation – Call Center Considerations

• Internal Concerns

- In many cases, organizations have issues with potential call volumes associated with a breach
- Call center need specialized training

• External Solutions

- Assistance and coordination with legal counsel to develop the optimal script and FAQ
- Dedicated toll-free number to be utilized solely for initial and follow up communications with victims
- Customer Contact Representatives specially trained with appropriate scripting to provide answers to victim's questions regarding the incident, the free credit monitoring product offered, Identity Theft in general, and/or your company using talking points provided by your company.
- Collecting information from caller as directed by your company to be provided to your company and/or credit monitoring agency as well as providing appropriate escalation information if needed to callers.
- Provide quality monitoring of calls as well as results in daily customized reports.
- The “hand off” to the credit monitoring or other company managing the loss mitigation solution is critical. It has been the source of problems for companies experiencing privacy breaches and it can lead to further brand damage

The Five Step Survival Guide



Communication & Remediation – Recovering Losses Through Contracts

- Indemnification
- Limitations of Liability
- Insurance
 - Limits / Retentions
 - Additional Insured Status
 - Waivers of Subrogation
 - Other Insurance
- Warranties
- Representations

The Five Step Survival Guide



Communication & Remediation – Recovering Losses Through Insurance

- **Crisis Management Expenses** - Covers the following expenses following a security breach
 - Forensic Expenses - Cost to investigate and establish the breadth of the loss
 - Public Relations – Costs to hire public relations firm to manage publicity associated with a privacy incident
 - Notification Costs – Cost to notify each party impacted by a security breach
 - Credit Monitoring – Cost to provide the parties impacted by a security breach with a 12 month credit monitoring package and a \$10,000 – \$25,000 identify theft insurance policy
 - Call Center – Cost to set up an emergency call center, develop a script and train personnel to handle calls from parties impacted by a security breach and profile identify theft assistance to victims
 - Credit Card Provider – Cost for complying with contractual terms with credit card providers including credit card re-issuance and associated fines and penalties
- **Privacy Liability** - Covers Third Party liability arising out of the following Perils:
 - Unauthorized access into your company computer system. Includes coverage for unauthorized disclosure of private information (name, credit card, social security number, etc);
 - Data theft;
 - Failure to protect private information in any medium (business, consumer or employee data) or the failure of third party vendor to protected private information under contract. Coverage should also extend to errors or omissions in compliance with your privacy policy (i.e. opt in or opt out errors)