

NEAL ■ GERBER ■ EISENBERG

Data Breaches: Lessons Learned and Guidelines for Developing an Incident Response Plan

Tenth Annual
Institute on
Privacy and Data
Security Law

July 20, 2009

© Neal, Gerber & Eisenberg LLP 2009



Diana J.P. McKenzie
Partner and Chair – Information
Technology Practice Group
Neal, Gerber & Eisenberg LLP
Office: (312) 269-8093
Cell: (847) 370-1121
dmckenzie@ngelaw.com
www.ngelaw.com

Roadmap

- Introduction
- Anatomy of a Security Breach
- Dealing with the Initial Emergency
- Ambiguities in State Laws
- Working with State Officials
- Do's and Don'ts of Notification Letters
- Incident Response Plans
- Post-Breach Issues

Introduction

- Breach notification laws: goals are straightforward
- Application is complicated
 - Patchwork of state laws
- Incidence response plan can prevent haphazard response
- Case study approach

Anatomy of a Security Breach

- Basic fact pattern
 - Electric utility based in North Carolina (NCE)
 - NCE had previously outsourced all customer care operations to “Old Vendor”
 - NCE recently switched to “New Vendor” for outsourcing of all customer care operations
- New Vendor discovers security breach during transition
 - Who did it?
 - What did they do?

Dealing with the Initial Emergency

- New Vendor and NCE work together to stop the fraud
 - Employee not immediately terminated, but put on leave and interviewed to obtain information
 - Private investigation firm hired
 - Employee's work computer and all of his emails were scrutinized
 - "Smoking gun" email was discovered
- Old Vendor and New Vendor conduct comprehensive security check

Dealing with the Initial Emergency

- Parallel step: determine NCE's obligations under the applicable breach notification laws
- Initially requires answers to “who, what, and for how long”
 - *Whose* information was breached?
 - *What* personal information was accessed?
 - For *how long* did the breach occur?
- In the ongoing investigation of an emergency, these questions can be difficult to answer
 - In NCE's case, answering “what” was easy
 - But “who” and “how long” proved difficult

Ambiguities in State Laws

- Which state's breach notification law applies?
- Some NCE customers only lived in North Carolina part of the year
 - Example: A few also lived in New York, and some of their electric bills were sent to New York
 - Did NCE therefore “conduct business” in New York for purposes of that state's breach notification law?
- Some former customers had moved to a different state
 - Which breach notification law applies, North Carolina or their new state of residence?
- NCE's Answer: when in doubt, work as though *both* state breach notifications laws apply
 - In the end, 12 state laws were at issue

Ambiguities in State Laws

- Varying notification requirements
 - Who must be notified (other than the customer)?
 - North Carolina: attorney general's office, but only if more than 1000 residents are affected
 - New York: attorney general's office plus additional state officials, even if only 1 resident is affected
 - Content of the notification letter
 - North Carolina: advice to “remain vigilant”
 - New York: no such requirement
 - Other variations: how to request a credit freeze (Mass.), steps taken to protect information from further unauthorized access (Virginia)

Ambiguities in State Laws

- Varying notification requirements (cont.)
 - Other ambiguities
 - Definition of “personal information”
 - Definition of “security breach”
 - Role of law enforcement
 - Timing of notice
- Result: “one-size-fits-most” approach
 - Draft notification letter that meets the requirements of most states, and treat “outlier” states separately
 - Sensible approach, but leads to doing more than legally necessary

Working with State Officials

- It may make sense to involve state officials early
 - NCE involved law enforcement early on
 - Police detective allowed NCE to lead investigation
 - If necessary, could have gotten a warrant for employees' home computer
- Reaching out to state officials early may have other benefits
 - Can help highlight mitigation / prevention efforts in the press
 - But proceed with caution – chief concern of state attorneys general is consumer protection

Do's and Don'ts of Notification Letters

- Distinguish between minimum legal requirements and good business sense
 - Avoid the fate of ChoicePoint
 - Only notified California residents, since that was the only state with a breach notification law at the time
 - Public backlash: stock tumbled 20% in 18 days
 - Fined \$15 million by the FTC
 - NCE notified Mississippi residents, even though that state lacked a breach notification law
 - Also hired a “people-finder” service to track down customers that had moved and changed their name

Do's and Don'ts of Notification Letters

- Similar issue with content of breach notification letter
 - Variations in the letter can lead to backlash
 - Study: companies are 4 times more likely to lose customers if they don't notify in a clear, *consistent*, and timely fashion
 - Supports the “one-size-fits-most” approach
- Consistency is necessary, but not sufficient
 - Same study: business 3 times more likely to lose customers if they used a form letter or email, rather than personalized letter or telephone call

Do's and Don'ts of Notification Letters

- Bottom line: most effective notification letter from a business (not necessarily legal) perspective
 - Personalized, written clearly
 - Accepts responsibility without making excuses or admitting fault
 - Provides assistance, useful information
 - Sends the message that the company is doing everything it can to protect the recipient of the letter
- Caution: letters may be made public
 - Some states (e.g., Maryland) publish notification letters on the web

Incident Response Plans

- Having an incident response plan can be very helpful in preparing for, and handling, a security breach
- NCE a good example – it lacked a plan, and at first its response was delayed and disorganized
 - Help desk supervisor who discovered the fraud didn't report it because he thought he “would get in trouble”
 - Response team that was established did not include members from important business units, such as marketing
 - Members of the team had never worked together
 - Certain employees with particular expertise were on vacation and could not be found

Incident Response Plans

- Many of these problems can be avoided through a *properly implemented* incident response plan
 - Designate a team that will own the plan
 - Place a senior manager in charge to give the team credibility and authority
 - Train employees
 - Test the plan through simulation of various types of breach
 - Plan should take into account vendor relationships

Post-Breach Issues

- Risk of class action lawsuits
 - Expected payoff must be high to justify the upfront risk
- Threatening letters
 - Emerging trend: law firms that specialize in responding to security breach notification letters
 - Typically, letters from these firms fail to tie the breach to actual harm
 - Engage in “fishing expeditions”
 - Mainly intended to secure a quick settlement and obtain information

Post-Breach Issues

- Generosity can serve as a shield to litigation
 - NCE: offered to pay the affected customers' fees for credit monitoring and credit fraud insurance
 - If accepted, any damages suffered as a result of the breach is reduced by the amount of insurance
 - If declined, the customer failed to mitigate damages
 - This would also reduce the damage award, if any
- Typically, only 10% to 20% accept these types of offers

Questions?

Diana J. P. McKenzie
Partner and Chair, Information
Technology Practice Group
Neal, Gerber & Eisenberg LLP
Office: (312) 269-8093
Cell: (847) 370-1121
dmckenzie@ngelaw.com
www.ngelaw.com