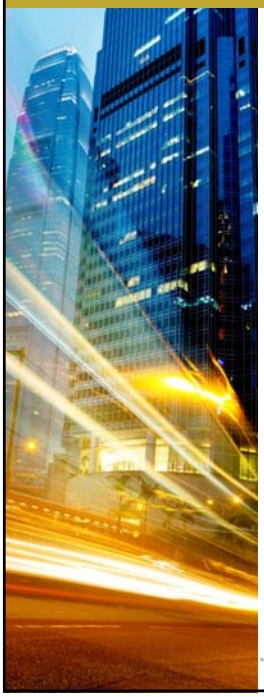
Katten

Katten Muchin Rosenman LLP

THE FIRST 48 HOURS:

Responding to a Data Breach in 2015



Anatomy of a Data Breach Response

The First 48 Hours

Panelists:
Claudia Callaway, Chair, Consumer Finance Litigation practice & Co-Chair, Class Action and Multidistrict Litigation practice
Christina Grigorian, Special Counsel, Financial Services practice

Chicago Moderator:
Megan Hardiman, Co-Head, Privacy, Data and Cybersecurity Group

New York Moderator:
Doron Goldstein, Co-Head, Privacy, Data and Cybersecurity Group

Katten
Katten Muchin Rosenman LLP

So…*What Happened?*

- Your employee installed music file sharing software on her company laptop.and consumer health files were stolen
- A credit card "skimmer" was installed on the computer in a restaurant at one of your hotels
- After much persistence, a hacker gained access to your sales website over a holiday weekend

Katten
Katten Muchin Rosenman LLP

1

Fact:

- What happens in the first 48 hours after you learn of a data breach is entirely dependent upon what you have done in the months and years leading up to the breach

Katten
Katten Muchin Rosenman LLP

2

Risk Mitigation: A Checklist

- Have we identified our "crown jewels"?
  - Warrant the most protection (DOJ)
- Do we conduct an ongoing assessment of security risk?
- Do we have security protocols and practices in place?
- Do we have privacy and security training?
- Do we have a strong vendor management program?
- Did Legal review all of our vendor indemnity and warranty protections?
- Have we done an insurance coverage assessment?
- Do we have an Incident Response Plan in place?
- Do we have a Notification and Communication Plan?
- Did Legal look at what our reporting obligations are?

Katten
Katten Muchin Rosenman LLP

3

Things to Keep in Mind…

- Follow the federal rules that apply to you (FTC, CFPB, OCC, FDIC, HHS, FCC)
- Regularly communicate policies to employees
- Consider a telecommuting/"bring your own device" policy
- Prevent terminated employees from accessing system
- Board and C-level buy-in

Katten
Katten Muchin Rosenman LLP

4

The Questions Go Like This…

- "Who's in charge here?"
- "What does our incident response plan say?"
- "Did we really have a breach?
- "Do we have a safe harbor?"
- "Who, exactly, do we have to notify?
- "When does the notification clock start ticking?"
- "What's out external notification plan?"
- "So…now what?"

Katten
Katten Muchin Rosenman LLP

5

…and the Consequences/Source of Stress Look Like This…

- Possibility of Negative Press Coverage
- Reputational Risk
- Loss of Business
- Underwriting "Demotion"/Industry "Write Down"
- Regulatory Investigations/ Enforcement Actions, Fines & Penalties
- Private Litigation
  - Individual or Class Action
    - Tort, Breach of Contract (Privacy Policy), UDAAP
  - Shareholder
  - Client

Katten
Katten Muchin Rosenman LLP

6

Materials to be Discussed

- Response Timeline
- Incident Response Plan Outline
- Safeguards Policy Outline
- Insurance Policy Checklist
- Notification Checklist

Katten
Katten Muchin Rosenman LLP

7

DATA BREACH TIMELINE – FIRST 48 HOURS AND BEYOND

Katten
Katten Muchin Rosenman LLP

8

General Timeline*

- Mobilize Team
  - Contact Outside Counsel/Engage Outside Experts
- Investigation**
- Secure/Mitigate**
  - Maintain records for forensic analysis
- Notify Law Enforcement
- Evaluate Insurance Options
- Determine Notice Requirements; Implement Communications Strategy
- Remediate/Retrain/Strengthen**
- Document

* These are not linear, and many are concurrent **Ongoing activities

Katten
Katten Muchin Rosenman LLP

9

An Ounce of Prevention…

- Big data breaches require crisis management
- Preparation is the best defense
  - Have a detailed Incident Response Plan in place before you are breached
    - Practice it regularly

Katten
Katten Muchin Rosenman LLP

10

1. "WHO'S IN CHARGE HERE?"

Katten
Katten Muchin Rosenman LLP

11

WHO's in Charge?

- Chief Information Officer, Chief Privacy Officer, Data Compliance Officer, etc.
  - Responsible for Policies, Procedures and Incidence Response Plan
  - Health Care: HIPAA
  - "Financial Institution": Gramm-Leach-Bliley Safeguard Policy
  - Telecom Industry: FCC Regulations
- Involvement of C-Suite Decision-Maker
- Legal Plays a Key Role

Katten
Katten Muchin Rosenman LLP

12

2. "WHAT DOES OUR INCIDENT RESPONSE PLAN SAY?"

Katten
Katten Muchin Rosenman LLP

13

Elements of an Incident Response Plan

- Identify Response Team
- Pre-Breach Documentation
- Steps for Immediate Mitigation
  - Contain Breach
  - Convene Response Team
  - Analyze Breach (Scope and Implications)
- Law Enforcement Contact Plan
- Insurance Contact Plan
- Identification of Jurisdictions & Statutes Involved
- Development of Notification Plan
- Communication Strategy: Internal, Regulatory, Public
- Draft Model Notices
- Post-Notification Plan
  - Follow-Up Plan
  - Litigation Plan
  - Audit Plan
  - Revisions to Incident Response Plan

Katten
Katten Muchin Rosenman LLP

14

3. "DID WE REALLY HAVE A BREACH?"

Katten
Katten Muchin Rosenman LLP

15

What is a "Breach"?

- Most states: the unlawful acquisition of personal information that compromises the security, confidentiality, or integrity of personal information
- Some states define a breach to include unauthorized access
- State and federal law definitions vary

Katten
Katten Muchin Rosenman LLP

16

What is "Personal Information"?

Basic State Law Definition: An individual's first name (or first initial and last name) **plus** one or more of the following data elements:

- Social Security number
- driver's license number or state issued ID card number
- account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account

But…most states have expanded on that, and federal laws have additional definitions of protected information

Katten
Katten Muchin Rosenman LLP

17

What is "Protected Health Information"?

- Individually identifiable health information in any form (oral, written, electronic, etc.) that relates to:
  - An individual's past, present or future physical or mental health or condition;
  - The provision of health care to the individual; or
  - The past, present or future payment for the provision of health care to the individual
- Includes demographic information (name, address, birth date, SSN)

Katten
Katten Muchin Rosenman LLP

18

What is a HIPAA "Breach"?

- *Any* impermissible acquisition, access, use or disclosure of PHI (limited exceptions)
- Presumed to be a breach unless "low probability of compromise" as determined by assessment of at least these factors:
  1. Nature and extent of PHI (e.g., financial, clinical)
  2. Unauthorized person obtaining PHI
  3. PHI actually acquired or viewed
  4. Extent to which risk mitigated (e.g., written assurance from recipient)

Katten
Katten Muchin Rosenman LLP

19

Not Just "Hacker" Incidents

- Stolen or misplaced laptop or flash drive
- Employee installation of file sharing software
- Employee emailing data to personal account
- In most – but not all – states data breach laws only apply to breach of computerized data
  - HIPAA applies to breaches of PHI in any form (written, oral, electronic)
  - Contractual requirements may be broader than state law

Katten
Katten Muchin Rosenman LLP

4. "DO WE HAVE A "SAFE HARBOR"?"

Katten
Katten Muchin Rosenman LLP

ENCRYPTION IS THE KEY

- Almost all breach laws provide a “safe harbor” where the compromised data is encrypted
  - Encryption = no consumer notification required
- Encryption standards: SSL and more
  - HIPAA: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html*

Katten
Katten Muchin Rosenman LLP

22

“What if it wasn’t encrypted?”

- Most states have a “risk of harm” analysis element that triggers/excuses notification
  - HIPAA no longer has a risk of harm standard

Katten
Katten Muchin Rosenman LLP

23

5. “WHO DO WE HAVE TO NOTIFY?”

Katten
Katten Muchin Rosenman LLP

Who do we have to notify?

- STATE LAW
  - Local Law Enforcement*
  - Consumers*
  - AG*
  - Other Regulator
- INSURER(S)
- CONTRACTUAL NOTICES
- FEDERAL LAW
  - Local Law Enforcement*
  - FBI
  - Other Regulator
- MEDIA
- NOTE: In some instances, law enforcement may ask you to “hold off” on notifying consumers
  - Get this in writing

Katten
Katten Muchin Rosenman LLP

How many states?

- Where is the company located?
- Where are the impacted systems located?
- Where are the affected consumers located?

Katten
Katten Muchin Rosenman LLP

Insurance Notification

- "Has legal reviewed our policies for data breach coverage?"
  - Look to policy notification timing requirements
  - Look to breach plan/incident response plan requirements
  - Look to federal/state/private action/regulatory coverage provisions
- Timing: too soon vs. too late

Katten
Katten Muchin Rosenman LLP

6. “WHEN DOES THE NOTIFICATION CLOCK START TICKING?”

Katten
Katten Muchin Rosenman LLP

28

Notification Timing

- Many states simply require “expeditious” notification
  - Some states have express time requirements for notification
- Balance between timely notification and getting all of the facts:
  - If the data was encrypted, you may not need to notify…
  - Get info on total number of affected consumers
  - Do a risk of harm analysis or other analysis as applicable
- Contracts may impose shorter timeframes

Katten
Katten Muchin Rosenman LLP

29

HIPAA Notification Basics

- Individual: No later than 60 days after discovery
- HHS:
  - 500 or more individuals – notice to HHS no later than 60 days after discovery
  - < 500 individuals – notice to HHS no later than 60 days after end of each calendar year, per HHS website
- Media: > 500 residents of state/jurisdiction – notice to prominent media outlet no later than 60 days after discovery
- Notice process depends on whether you are a Covered Entity or a Business Associate

Katten
Katten Muchin Rosenman LLP

30

7. "WHAT'S OUR EXTERNAL NOTIFICATION PLAN?"

Katten
Katten Muchin Rosenman LLP

31

Notification Checklist

- Law Enforcement
- Insurance
- Regulators
- Vendors
- Customers
- Media
  - Website?

Katten
Katten Muchin Rosenman LLP

32

Messaging is Critical

- Check legal requirements for special content and timing requirements
  - Law enforcement may want to keep certain data out of public record
- Have outline of press response in the Incident Response Plan
- Approve call center scripts/FAQs for affected individuals and customers
- Consider shareholder notification

Katten
Katten Muchin Rosenman LLP

33

8. “NOW WHAT?”

Katten
Katten Muchin Rosenman LLP

RISK OF LITIGATION & ENFORCMENT ACTIONS

- Risk of Private Litigation
  - State common law tort and contract theories
  - Some state data breach statutes provide for private right of action
  - GLBA/federal law violations
  - Shareholder action
- Risk of Regulatory Action
  - Federal regulators
    - FTC, CFPB, FCC, HHS/OCR/DOJ, SEC, FDIC, OCC
  - State
    - AG, DOI, etc.
  - Potential for significant civil penalties/fines and enforcement

Katten
Katten Muchin Rosenman LLP

RISK OF LITIGATION

- "Do we have an arbitration agreement/class action waiver in our customer agreements?"
  - A fair individual arbitration provision/class action waiver is enforceable
    - *AT&T v. Concepcion*
  - CFPB currently "looking at" use of such provisions in consumer finance agreements

Katten
Katten Muchin Rosenman LLP

36

HIPAA Civil Monetary Penalties

- Civil monetary penalties of up to $50,000 per violation, up to $1.5 million for all identical violations in a calendar year
- Often resolved through Resolution Agreements with (settlement payment plus multi-year Corrective Action Plans)
  - These can be very costly
- Possible follow-up investigations
  - OCR: automatic if breach > 500 individuals
- You will have the burden of proof that notice was given, or was not required

Katten
Katten Muchin Rosenman LLP

37

POST-INCIDENT STEPS

- Identify lessons learned
- Take steps to prevent future recurrence
  - Revise Policies, Procedures
  - Train and Re-Train
  - Practice/Refine your Incident Response Plan
  - Evaluate Your Vendor Management Program
  - Review/Adjust Allocation of Security Budget
- Document steps taken
  - Retain required documentation

Katten
Katten Muchin Rosenman LLP

38

Q&A

Katten
Katten Muchin Rosenman LLP

39

Katten Muchin Rosenman LLP Locations

AUSTIN
One Congress Plaza
111 Congress Avenue
Suite 1000
Austin, TX 78701-4073
+1.512.691.4000 tel
+1.512.691.4001 fax

HOUSTON
1301 McKinney Street
Suite 3000
Houston, TX 77010-3033
+1.713.270.3400 tel
+1.713.270.3401 fax

LOS ANGELES – CENTURY CITY
2029 Century Park East
Suite 2600
Los Angeles, CA 90067-3012
+1.310.788.4400 tel
+1.310.788.4471 fax

ORANGE COUNTY
100 Spectrum Center Drive
Suite 1050
Irvine, CA 92618-4960
+1.714.966.6819 tel
+1.714.966.6821 fax

WASHINGTON, DC
2900 K Street NW
North Tower - Suite 200
Washington, DC 20007-5118
+1.202.625.3500 tel
+1.202.298.7570 fax

CHARLOTTE
550 South Tryon Street
Suite 2900
Charlotte, NC 28202-4213
+1.704.444.2000 tel
+1.704.444.2050 fax

IRVING
545 East John Carpenter Freeway
Suite 300
Irving, TX 75062-3964
+1.972.587.4100 tel
+1.972.587.4109 fax

LOS ANGELES – DOWNTOWN
515 South Flower Street
Suite 1000
Los Angeles, CA 90071-2212
+1.213.443.9000 tel
+1.213.443.9001 fax

SAN FRANCISCO BAY AREA
1999 Harrison Street
Suite 700
Oakland, CA 94612-4704
+1.415.293.5800 tel
+1.415.293.5801 fax

CHICAGO
525 West Monroe Street
Chicago, IL 60661-3693
+1.312.902.5200 tel
+1.312.902.1061 fax

LONDON
Paternoster House
65 St Paul's Churchyard
London EC4M 8AB United Kingdom
+44.0.20.7776.7620 tel
+44.0.20.7776.7621 fax

NEW YORK
575 Madison Avenue
New York, NY 10022-2585
+1.212.940.8800 tel
+1.212.940.8776 fax

SHANGHAI
Suite 4906 Wheelock Square
1717 Nanjing Road West
Shanghai 200040 P.R. China
+86.21.6039.3222 tel
+86.21.6039.3223 fax

Katten
Katten Muchin Rosenman LLP
www.kattenlaw.com