Data Breaches

Legal and IT Responses

KUTAK ROCK LLP

Todd Kinney

& Bruce Wray

Kutak Rock – Omaha

Introduction to Data Breaches

IT Response:

- Identify
- Contain
- Eradicate
- Recover
- Debrief

Legal Response:

- Identify Internal/External Teams
- End Incident
- Engage Outside Resources (forensics, law enforcement, insurance)
- Assess Exposure
- Update Logs
- Analyze Incident
- Issue Breach Notifications

KUTAK ROCK LLP

Legal Response

Identify Internal/External Teams

Who:

- Internal managers and possibly executives
- Required IT resources
- External legal counsel

Start Considering?

- Law enforcement
- Insurance
- Call Center

Why:

- Smaller, surgical team to debrief and manage incident
- Executive authority to engage and make decisions
- Internal and/or external legal team to assess exposure

KUTAK ROCK LLP

End Incident

- Relying upon IT resources
- Collection of data and evidence for legal and law enforcement
  - Forensic evidence
- Determine scope:
  - Whose data was lost?
  - Type of data?
  - Content of data?
  - Who holds the data?
  - State of origin of data?

KUTAK ROCK LLP

Engage Outside Resources

These may include:

- Forensics teams
- Law enforcement
- Insurance
- Call Center

Insurance notes:

- Promptly notify and follow notification requirements in policy
- Provider may restrict who and when others can be engaged

KUTAK ROCK LLP

Assess Exposure

Tied to outcome of IT resources work

- Which accounts, software, networks, servers, and/or physical space was exposed?
- What states were affected individuals from?
- Was any Personally Identifiable Information* (PII) exposed?

Assess Exposure – Why By State?

Goal – Determine if there was a breach that requires notification

Why ask what states were affected individuals from:

- Some notifications and definitions are federal, meaning there is one set of definitions, requirements, and notifications across the country
- States, however, also have varying statutes, with different definitions and notifications

KUTAK ROCK LLP

Assess Exposure – Why By State?

Goal – Determine if there was a breach that requires notification

State by State to Determine:

- Which statutes need to be examined
- What definition of Personally Identifiable Information governs
- What definition of Breach governs
- What notifications are required

KUTAK ROCK LLP

Assess Exposure – What is PII?

Goal – Determine if there was a breach that requires notification

General Definition

- **Personally identifiable information** (**PII**), or sensitive **personal information** (SPI), as used in **information** security and privacy laws, is **information** that can be used on its own or with other **information** to identify, contact, or locate a single person, or to identify an individual in context. (source: Wikipedia)

KUTAK ROCK LLP

10

Assess Exposure – What is PII?

Goal – Determine if there was a breach that requires notification

Alaska's Definition of PII:

(7) "personal information" means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of

- (A) an individual's name; in this subparagraph, "individual's name" means a combination of an individual's
  - (i) first name or first initial; and
  - (ii) last name; and
- (B) one or more of the following information elements:
  - (i) the individual's social security number;
  - (ii) the individual's driver's license number or state identification card number;
  - (iii) except as provided in (iv) of this subparagraph, the individual's account number, credit card number, or debit card number;
  - (iv) if an account can only be accessed with a personal code, the number in (iii) of this subparagraph and the personal code; in this sub-subparagraph, "personal code" means a security code, an access code, a personal identification number, or a password;
  - (v) passwords, personal identification numbers, or other access codes for financial accounts.

Sec. 45.48.090. Definitions.

KUTAK ROCK LLP

11

Assess Exposure – What is PII?

Goal – Determine if there was a breach that requires notification

Alaska's Definition of Breach:

(1) "breach of the security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector; in this paragraph, "acquisition" includes acquisition by

(A) photocopying, facsimile, or other paper-based method;

(B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or

(C) a method not identified by (A) or (B) of this paragraph;

Sec. 45.48.090. Definitions.

KUTAK ROCK LLP

12

Assess Exposure – What is PII?

Goal – Determine if there was a breach that requires notification

Nebraska's Definition of PII:

(5) Personal information means either of the following:

- (a) A Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:
  - (i) Social security number;
  - (ii) Motor vehicle operator's license number or state identification card number;
  - (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account;
  - (iv) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or
  - (v) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or
- (b) A user name or email address, in combination with a password or security question and answer, that would permit access to an online account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records

Nebraska Revised Statute 87-802

KUTAK ROCK LLP

13

Assess Exposure – What is PII?

Goal – Determine if there was a breach that requires notification

Nebraska's Definition of Breach:

(1) Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system;

Nebraska Revised Statute 87-802

KUTAK ROCK LLP

14

Assess Exposure – Not just PII?

Goal – Determine if there was a breach that requires notification

This analysis does not begin or end with PII, under it's varying definitions

- Some states have solo statues targeted at Social Security Numbers, drivers IDs
- HIPAA, PCI, etc.

KUTAK ROCK LLP

15

Assess Exposure – Not just PII?

Goal – Determine if there was a breach that requires notification

HIPAA governs:

- Personal Health Information
- Varying degrees of “anonymization” allowed
  - Example – age plus zip may individually identify

PCI governs:

- Card and Cardholder Data

KUTAK ROCK LLP

16

Update Logs

Two types:

- Physical Logs and Electronic Logs leading up to and including incident
- Response Logs maintained throughout the process
  - Excel Spreadsheet with tasks, timelines, and signoffs
  - May require adjustment throughout process

KUTAK ROCK LLP

17

Analyze Incident

Goal – Determine if there was a breach that requires notification

Steps:

- Was there a “breach” as defined by applicable statute?
- Are the notifications requirements triggered?
- Who must be notified – individuals, attorney(s) general, governmental agencies?
- Deadlines for notification letters?

KUTAK ROCK LLP

18

Issue Breach Notifications

Goal – Determine if there was a breach that requires notification

We have to notify, now what?

- What are requirements of notification, and to whom?
- Will we engage a Call Center to assist and which one?
- Are there other services we want to offer those affected?
  - Credit Monitoring
  - Fraud Protection

KUTAK ROCK LLP

19

Other Breach Issues

Other Breach Issues – Vendor Breach vs Internal Breach

- Vendor Breach
  - Contract Terms Often Govern
  - Do they notify you?
  - What do they share?
  - How do they share?
  - When do they share?
- Internal Breach
  - All response responsibility lies with you

KUTAK ROCK LLP

21

Other Breach Issues – Insurance

Insurance:

- Can be expensive, but defrays costs during incident
- May dictate approved providers and available steps
- May not match legal requirements
  - i.e. you may be legally obligated to do more than they are contractually obligated to pay for

KUTAK ROCK LLP

22

Thank you.

Todd Kinney, Partner
Intellectual Property & Information Practice Group
Kutak Rock – Omaha
Todd.Kinney@KutakRock.com
(402) 346-6000

Bruce Wray, Associate
Intellectual Property & Information Practice Group
Kutak Rock – Omaha
Bruce.Wray@KutakRock.com
(402) 346-6000