DATA BREACH NOTIFICATION

Abigail Stempson  
Nebraska  
Chief, Consumer Protection Division

Alissa Gardenswartz  
Colorado  
Deputy AG, Consumer Protection Section
AGENDA

- Overview
- Anatomy of a Data Breach
- State Data Breach Notification Laws
- Liability
- Prevention
- Actions Following a Breach
- Working With Your Attorney General
- Questions
OVERVIEW

- With charitable giving exceeding $373 billion in 2015, charities are increasingly becoming targets of data security attacks.
  - *Giving USA’s Annual Report on Philanthropy for the Year 2015*

- Sensitive information that is of interest to hackers goes well beyond a credit card number: User names, email addresses, physical addresses, passwords, etc.

- Donors are becoming more concerned about the protection of their personal and financial information.
ANATOMY OF A DATA BREACH

- **Accidental Disclosure**: This can include a well-meaning insider, loss of a device, sending e-mail to the wrong person, etc.

- **Targeted Attacks**: Cyber-criminals using malicious code that can penetrate undetected and export data. This is made possible by:
  - System vulnerabilities
  - Improper credentials
  - Targeted malware
  - Spyware
  - Phishing

- **The Malicious Insider**: Insiders who knowingly steal data.

- **Compromised Vendor**: Provides auxiliary support but receives third-party sensitive information. Not the primary target of the hack.
DATA BREACH STATISTICS - 2015

- 780 data breaches
  - Only includes breaches that have a name plus a Social Security number, driver’s license number, medical record, or financial record (credit/debit cards included).

- Over 177 million records accessed

- $7.01 million is the average total cost of a data breach.
  - $221 average cost per lost or stolen record.
  - Source: Ponemon Institute – 2016 Cost of Data Breach Study: United States
    - Note: the data breaches analyzed in the study involved between 5,000 and 100,000 records
WHAT IS A DATA BREACH?

- **Breach of Security:** The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information.

- **Common Definition of Personal Information**
  - An individual’s first name (or initial) and last name plus one or more of the following:
    - Social Security Number
    - Driver’s license number or state-issued ID card number
    - Account number, credit or debit card number, combined with any security code, access code, PIN or password needed to access an account

- **Additional Categories**
  - Medical history or health information
  - Biometric information
  - Email address and password
  - Tax ID number
STATE DATA BREACH NOTIFICATION LAWS

- **Time-Sensitive Notification**: States have differing requirements on when and how notifications must be sent out to individuals.

- **Notice to the state Attorney General**: Some states require a notice be sent to the state Attorney General or a State Agency informing them of a breach.

- **Risk of Harm Analysis**: Some states allow for exceptions to their notification requirements upon an assessment of the risk of harm to the affected individuals.

- **Encryption Safe Harbor**: States have different laws affecting the definition of a breach and the notification requirements based on whether the data was encrypted.

- **Paper or Electronic**: States also differ as to whether their laws affect only electronic materials, paper materials, or both.
10 STATES REQUIRE NOTIFICATION WITHIN A SPECIFIC TIME FRAME

Maine

- If, after the completion of an investigation, notification is required under this section, the notification required by this section may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.

Ohio

- Notice must be provided in the most expedient time possible but not later than 45 days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities.
28 STATES REQUIRE NOTICE TO ATTORNEY GENERAL OR STATE AGENCY

**Nebraska**
- If notice of a breach of security is required to be provided to affected individuals, the person must also provide notice of the breach to the Attorney General not later than the time when notice is provided to residents.

**New Jersey**
- The Division of State Police in the Law Department of Law and Public Safety must be notified regarding a breach prior to notifying customers.
States that Require Notice to a State Agency

- **Notification Required**
- **Notification NOT Required**
- **No Notification Law**
40 STATES REQUIRE RISK OF HARM ANALYSIS

Colorado

- Notification is NOT required if after a good-faith investigation, the entity determines that misuse of personal information about a Colorado resident has not occurred and is not likely to occur.

Virginia

- Notification required if the entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.
States the Require Risk of Harm Analysis

Risk of Harm Analysis
No Risk of Harm Analysis
No Notification Law
46 STATES WITH AN ENCRYPTION SAFE HARBOR

Iowa

- The statute does not cover personal information if it is “encrypted, redacted, or otherwise altered in such a manner that the name or data elements are unreadable” unless the keys to unencrypt, unredact, or otherwise read the data have been obtained through a breach of security.

Missouri

- Personal information does not include information that is redacted, altered, or truncated such that no more than five digits of a social security number or the last four digits of a driver’s license number, state identification card number, or account number is accessible as part of the personal information.

Note: Tennessee removed the safe harbor in 2016
States with an Encryption Safe Harbor

- Safe Harbor
- Removed Safe Harbor
- No Notification Law
8 STATES TRIGGERED BY A BREACH IN ELECTRONIC AND/OR PAPER RECORDS

**Alaska**

- “Breach of security” means unauthorized acquisition.
  “Acquisition” includes: acquisition by photocopying, facsimile, or other paper-based method; a device including a computer, that can read, write or store information that is represented in numerical form; or a method not identified by this paragraph.

**Hawaii**

- This statute applies to . . . any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes.
States Where Notification is Required in Breaches of Paper Records
LIABILITY FOR A SECURITY BREACH

- Individual Claims
  - Negligence
  - Negligent Misrepresentation
  - Contract Law Claims
  - Breach of Fiduciary Duty Claims
- Regulator Claims
  - Consumer Protection Act
  - Uniform Deceptive Trade Practices Act
PREVENTING A SECURITY BREACH
PREVENTION

- Take stock: Know what personal information you have in your files and on your computers.
- Scale down: Keep only what you need for your organization.
- Lock it: Protect the information that you keep.
- Pitch it: Properly dispose of what you no longer need.
- Plan Ahead: Create a plan to respond to security incidents.
Take Stock

- Assess what information you have and identify who has access to it.
  - Who sends or provides sensitive personal information to your organization?
  - How is this information received?
  - Where is this information stored?
    - Computers
    - Flash drives
    - Home computers
    - Cell phones
  - Who has – or could have – access to the information?

- Pay particular attention to how you keep personal identifying information: social security number, credit card or financial.
If you don’t have a legitimate business need for sensitive personal identifying information, don’t keep it.

- Don’t use Social Security Numbers unnecessarily, e.g. as an employee or customer identification number. Use SSNs only for required and lawful purposes like reporting employee taxes.
- Don’t keep customer or donor credit card information, e.g. account number, expiration date, card verification value code. It raises the risk it could be used to commit fraud or identify theft.
- Check default settings on software that read customers’ credit card numbers and processes transactions. Sometimes it is preset to keep information permanently.

Develop a written records retention policy to determine what information needs to be kept, how, for how long.
LOCK IT: PHYSICAL SECURITY

- Many data compromises happen the old fashioned way – through lost or stolen paper documents or storage devices.
  - Store paper documents, files, zip drives, etc., in locked storage areas.
  - Do not leave papers with sensitive information on your desk if away from work area.
  - Put files away, log off computers, lock file cabinets and office doors at the end of the day and when away from the office.
  - If you maintain off-site storage facilities, limit access to employees with legitimate business needs.
  - If you ship sensitive information, encrypt it, keep an inventory of the information shipped, and use an overnight shipping service that allows you to track delivery.
LOCK IT: ELECTRONIC SECURITY

- Understand the vulnerabilities of your computer system; follow the advice of experts in the field.
  - Identify the computers or servers where sensitive personal information is stored.
  - Identify all connections to these computers:
    - Electronic cash registers
    - Remote or branch office computers
    - Internet
    - Wireless devices including cell phones
  - Do not store sensitive information on computers with internet connections
  - Encrypt sensitive information you send to third parties over public networks.
  - Regularly run and update anti-virus, anti-spyware, and firewall to protect against known threats.
  - Use strong passwords with letters, numbers, and characters.
PITCH IT

- Implement disposal practices that are reasonable and appropriate.
  - “Reasonable and appropriate” is based on sensitivity of the information, costs and benefits of different disposal methods, and changes in technology
- Paper records – shred.
- Computers – wipe utility programs.
- Employees working from home should follow same procedures.
- If you use consumer credit reports for business purposes, you may be subject to the FTC’s Disposal Rule. (www.ftc.gov/privacy)
- Other devices
  - Copy machines
  - Printers
  - Cell phones
PLAN AHEAD

- Have plan in place to respond to security breaches.
- Investigate issues immediately.
- Consider whom to notify inside – and outside – your organization:
  - Clients/customers, patrons, donors
  - Law enforcement
  - Credit bureaus
  - Other businesses
SECURITY BREACH . . . NOW WHAT?
SECURITY BREACH PROTOCOL

- Once a breach is recognized, contain it.
  - Shut down accounts
  - Revoke user access
  - Make sure laptops and hand held devices have installed on them remote wipe technology
  - Deactivate laptops and devices

- Engage a 3\textsuperscript{rd} party data breach expert
- Determine the scope of the breach
- Implement notification requirements
WORKING WITH YOUR ATTORNEY GENERAL

- Attorney General
  - Outreach/Education
  - Penetration Testing
  - Data Security Guides

- Your Organization
  - Contacting our office before a breach
  - Reach out to us when a breach occurs
  - Develop standards and expertise