Data Privacy and Security for Businesses

Rotary Club of Brooksville
June 10, 2014

Tatiana Melnik
Melnik Legal PLLC
tatiana@melniklegal.com | 734-358-4201

Why?

- Why is there a spotlight on data security?

Data Breaches + Identity Theft = Liability

Data Breaches	Identity Theft
Target – 70 million records; 40 million cards; 100+ lawsuits; investigations by AGs, FTC	Florida number one state for various types of fraud, including identity theft
HIPAA related breaches – impacting more than 31 million individuals; class actions; government investigations	Types: Tax fraud, credit card, phone/utilities, bank, etc.
	Identity Theft = Damages

Why?

- Higher penalties, more investigations
- Office of Civil Rights most active, 18 settlements since 2011

Entity	Amount	Rules	Breach	Incident	Settlement
UCLA Health System	$865,500	Privacy & Security Rules	Workers snooping on celebrity patients	Prior to 6/5/2009	7/5/2011
Alaska Dept. of Health & Human Services	$1.7M	Privacy & Security Rules	unencrypted portable media device stolen from car of employee	10/12/09 (self reported)	6/25/2012
Affinity Health Plan	$1,215,780	Privacy and Security Rules	returned copiers to a leasing agent w/o erasing the copier hard drives	Prior to 4/15/10 (self reported)	8/7/2013

Who Has Obligations?

- Every business
  - Regulated
    - Healthcare – HIPAA – HHS's Office of Civil Rights, State AGs
    - Financial services – GLBA – Office of the Comptroller of the Currency, Federal Reserve Board, FDIC, etc.

Who Has Obligations?

- Every business
  - Non-Regulated
    - Federal Trade Commission
      - "works for consumers to prevent fraudulent, deceptive, and unfair business practices"
      - has authority to pursue **any company** that has engaged in "***unfair or deceptive acts or practices*** in or affecting commerce"
      - FTC settlement
        - 20 year compliance period
        - will take action against individual owners

Who Has Obligations?

- Every business
  - Non-Regulated
    - Florida Information Protection Act (SB 1524)
      - Unanimously approved by the legislature on April 30
      - Governor's signature pending
      - Broadens Florida's existing data breach law
      - Requires that "[e]ach covered entity, governmental entity, or third-party agent ***shall take reasonable measures*** to protect and secure data in electronic form containing personal information."

Who Has Obligations?

- Florida Information Protection Act
  - **Covered entity** = sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that **acquires**, **maintains**, **stores**, or **uses** personal information.
  - **Personal information** = means an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
    - SSN; driver license or identification card number; credit or debit card no. (w/security code, access code, password); healthcare information; individual's health insurance policy number; etc.

"Reasonable Measures"?

- What does it mean to "***take reasonable measures*** to protect and secure data in electronic form containing personal information"?
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards

And a Few More Questions…

Any Questions?

Tatiana Melnik
734.358.4201
tatiana@melniklegal.com

Disclaimer

This slide presentation is informational only and was prepared to provide a brief overview of some data privacy and security issues. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you on these matters.