UNIVERSITY of DAYTON

The Recent ID Theft Red Flag Regulations and Other Indicators to Help Organizations Build Defensible Data Protection and Compliance Programs

June 6, 2008

Oscar Marquis

- General Counsel of Trans Union
- Responsibilities
  - Compliance
  - Contracts
  - Government affairs
  - Regulatory issues

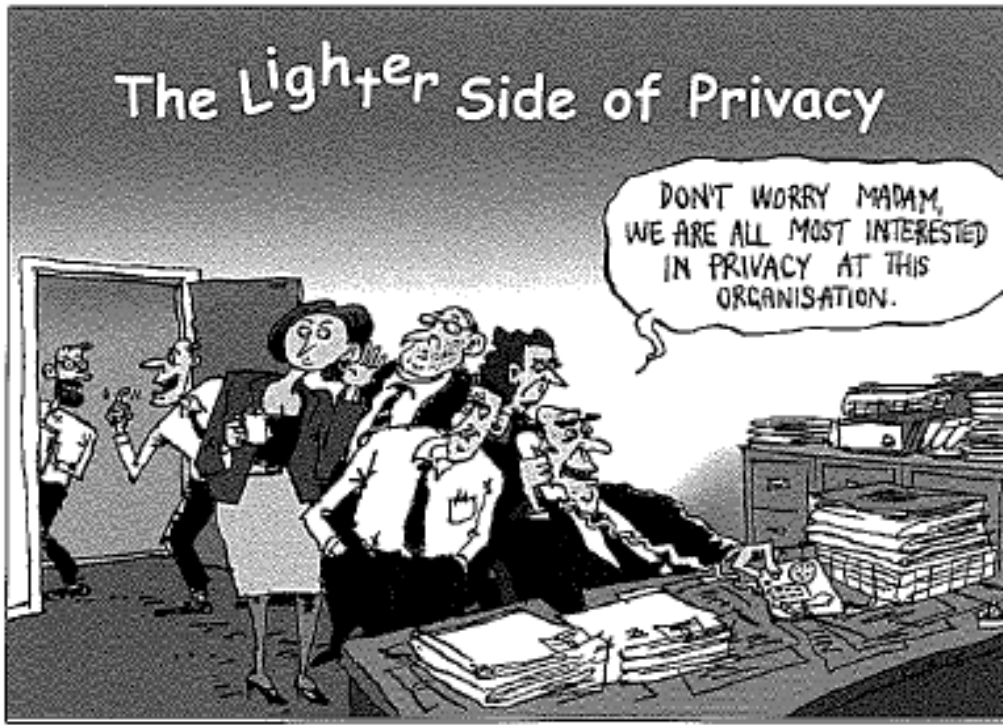
TRUSTED WISDOM. EXTRAORDINARY RESULTS.

RONALD I. RAETHER, JR.

- High-technology and privacy litigation, throughout the United States:
  - Federal and State Privacy Statutes
  - Trademark/Domain name disputes
  - Privacy/Data Security Assessments
  - Antitrust
  - Software/Hardware Product Performance

- Author and featured speaker on numerous technology and privacy related issues

Why Data Compliance Is Important….



Trusted wisdom. Extraordinary results.

2005
"A Coming Out Year"

- Year of the Security Breach
  - Over 160 Announcements (2/15/05 – 5/12/06)
  - 55 Million People

- Privacy and Compliance Issue

TRUSTED WISDOM. EXTRAORDINARY RESULTS.

Largest Incidents Since 2004

Number	Affected Date	Companies
94,000,000	2007-01-17	TJX Companies Inc.
40,000,000	2005-06-19	Visa, CardSystems, Mastercard, American Express
30,000,000	2004-06-24	America Online
26,500,000	2006-05-22	U.S. Dep't of Veterans Affairs
25,000,000	2007-11-20	HM Customs and Revenue
8,637,405	2007-03-12	Dai Nippon Printing Company
8,500,000	2007-07-03	Fidelity National Info Services
6,300,000	2007-09-14	TD Ameritrade
6,000,000	2008-05-11	Chilean Ministry of Education
5,000,000	2003-03-06	Data Processors International

TRUSTED WISDOM. EXTRAORDINARY RESULTS.

Most Recent Incidents

Number	Affected Date	Companies
13,000	2008-05-12	Pfizer
6,000,000	2008-05-11	Chilean Ministry of Education
103	2008-05-09	Princeton University Tower Club
5,000	2008-05-08	Dominican University
1,800	2008-05-08	Las Cruces Public Schools
159,000	2008-05-07	HSBC
Unknown	2008-05-06	Northeast Security
192	2008-05-06	Ohio State University ATI
2,000	2008-05-04	Westpac Banking Corporation
468	2008-05-02	Iredell County Tax Admin

Overview of 2007

Category	Business	Education	Medical	Government	Total
Number of Breaches	129	111	65	110	410
Consumers Affected	106,544,377	1,184,575	4,055,233	8,156,682	120 Million

Potential Cost of Breach

- 45.7 Million Records
- Internal Costs: $17 Million (June 17, 2007)
- $107 Million Reserve: 10Q for 2nd Q 2008
- FTC Settlement Announced March 2008
- Consumer Class Settles: $30-$80 Store vouchers: Sept. 2007
- Bank Lawsuits Pending
- Reputation/Consumer Confidence

Preparing for a Breach

- Assessment of Applicable Laws
- Understand Government and Trade Standards
- Have Good Protocols
- Assess Compliance

TRUSTED WISDOM. EXTRAORDINARY RESULTS.

Navigating Clients Through Regulatory Patchwork

You Don't Know What You Don't Know

- 2003 Fair and Accurate Credit Transactions Act
  - Amendment to FCRA
  - Prohibits certain credit card
  - Effective December 2006
  - Statutory Damages of $100 to $1000
- Class Actions – Hundreds filed in 2007
- Merchants still not in compliance
  - eCommerce

FCRA Objectives

- Accuracy
  - Consumer disclosure
  - Includes Inquiries
- Fairness
  - Limit reporting of information
- Privacy
  - Permissible purposes
  - Credential Users

Are You covered?

- Furnish Consumer Information
- For determining a Consumer's Eligibility For
  - Credit
  - Insurance
  - Employment
  - Other Permissible Purpose
- Excludes Transaction Information

New Focus—Privacy

- Permissible Purpose
- Credential Users of Information
- Security Procedures
- Chief Privacy Officer
- In order to Prevent—Identity Theft

Identity Theft

- Ever expanding crime.
- Easy to commit.
- The risk of getting caught is low.
- It can be committed in the privacy of your home.
- The actual victim is a big institution.
- All you need is a computer with internet access.
- The pay off can be substantial.

Identity Theft

- A unique crime
- There are two victims:
  - a financial institution whose money the criminal steals, and
  - a consumer whose identity is used.

Identity Theft

- A certain level of losses are expected.
- Some consumers loans are written off.
- They are calculated into the price—the interest rate.
- The percentage of expected losses is considered when loans are made regardless of the cause of the losses—bad credit risk or fraud

Legislation

- It was inevitable that Congress would try to stop this crime with legislation.
- Usually, legislation to stop a crime deals with the criminal—longer sentences, swifter prosecution.
- With identity theft, the legislation addresses one of the victims—and a third party: the credit bureau.
- Most of the obligations and costs in legislation fall on the credit bureaus.
- The Fair and Accurate Credit Transactions Act of 2003—Added Obligations

Red Flag rules

- FACT Act required
- Promulgated by FTC and Financial Regulatory Agencies
- Opening Accounts and Existing Accounts
- Guidelines to detect, prevent, and mitigate Identity Theft
- Effective November 2008

Red Flag Rules

- All About Identifying Risk
  - Recognize Risk
  - Control Risk
  - Establish Response Program
- Red Flags are 26 Risk Factors to Consider

Red Flag Rules

- Implement ID Theft Prevention Program
- Card Issuers to Verify Change of Address Requests
- Users of Consumer Reports and Address Variation Notice

Red Flag Rules

- Rules Include Things You Must Do,
- You Should Do
- And 26 Red Flags as Guidance

Red Flag Rules

- Program Must Be in Writing
- The Plan Must be Updated as Warranted
- Applies to Consumer and Business Accounts

Red Flag Rules

- Program:
  - Determine Which Accounts Are Covered
  - Determine Which Red Flags Apply
  - Establish Controls Relating to those Red Flags
    - Administrative
    - Technical
  - Appropriate Response to Controld
    - Close Account
    - Monitor Account

Red Flag Rules

- Red Flags (Examples)
  - Warnings from CRA
    - Fraud Alert on Consumer Report
    - Unusual Number of New Accounts on CR
    - Accounts Closed by Financial Institution
  - Suspicious Documents
    - Appear to be Forged or Altered
    - Photo is Inconsistent with Appearance

Red Flag Rules

- Red Flags (Examples)
  - Suspicious Personal Identifying Information
    - Address doesn't match CR
    - Bad correlation between SSN and DOB
    - Phone number matches others
  - Unusual Activity on Account
    - Change of Address followed by request for new card
    - Most available credit used for cash advances

Red Flag Rules

- Red Flags are for Illustrative Purposes, nnot Hard and Fast Requirements
- Aimed at Smaller FIs that are not as Sophisticated
- Flexible—Not a template
  - Recognize Risk
  - Promote creativity
  - Technologically neutral

Red Flag Rules

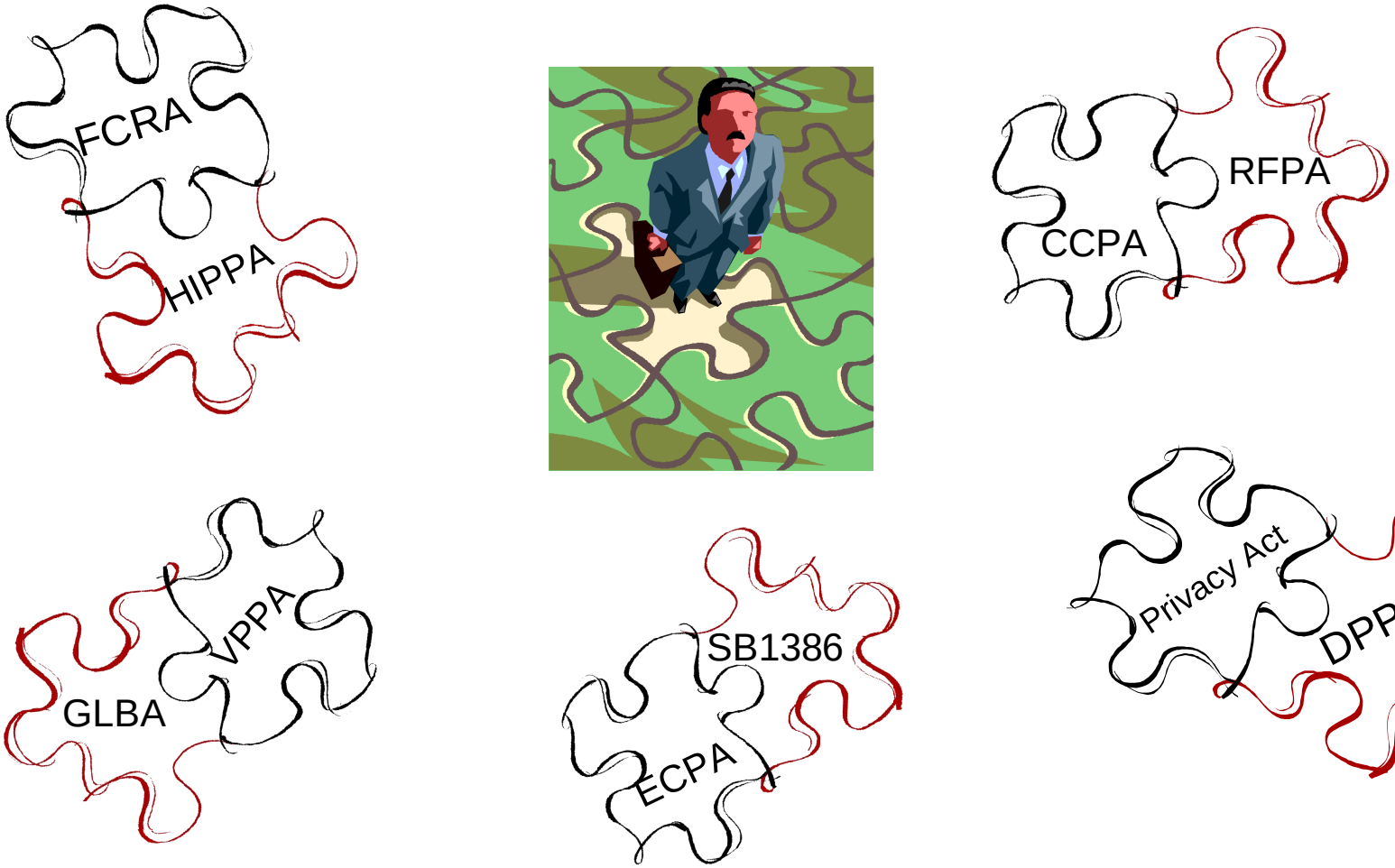
- Document What is not Used
- Point is—Recognize, Anticipate, Mitigate and Change based on Risk

Red Flag Rules

- Establish Procedures for Change of Address
  - Validate
  - Notify at former address
  - Easy manner of reporting incorrect address
- Establish Procedure for Address Discrepancy Notice from CRA
  - Use third party source
  - Verify

TRUSTED WISDOM. EXTRAORDINARY RESULTS.

Navigating Clients Through Regulatory Patchwork



Privacy In The Workplace

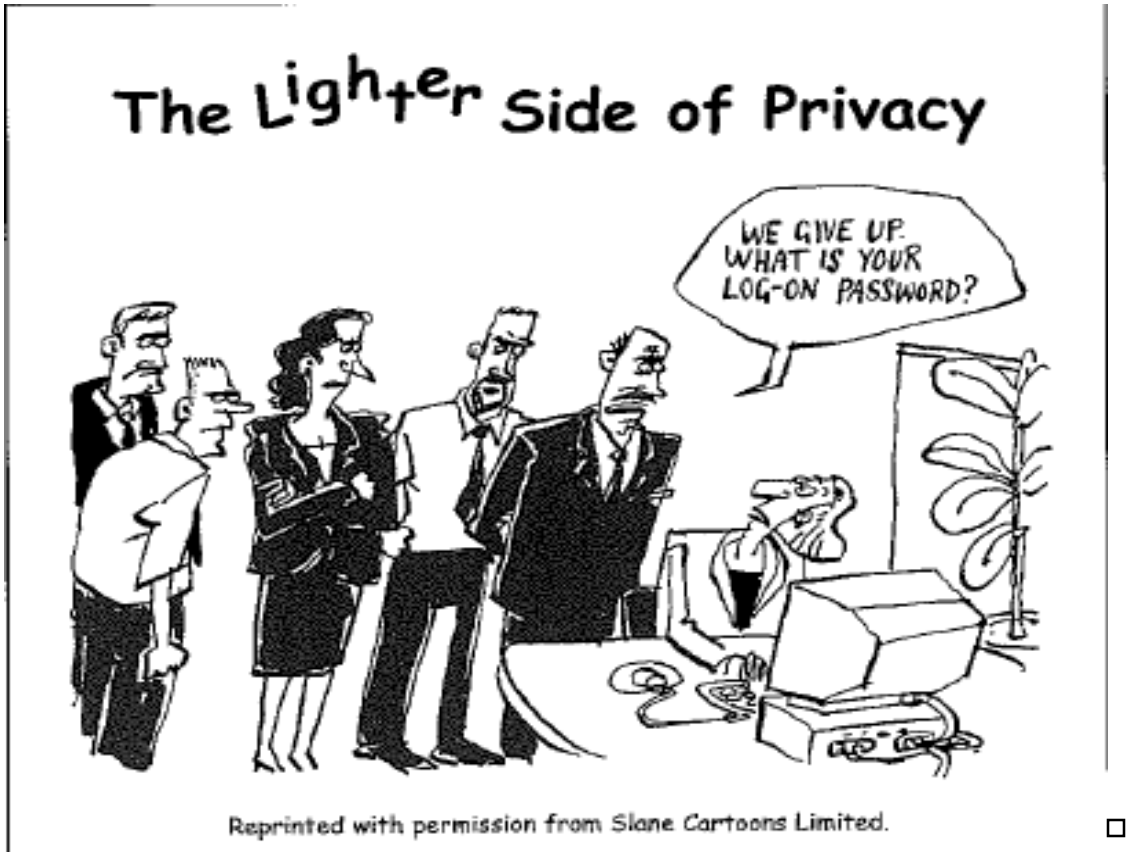
- Background Screening
- Employee Monitoring
  - Electronic Communications Privacy Act
  - Exceptions
- EU Data Protection Directive
- Sarbanes-Oxley compliance
- Social Security Number Laws

Preparing for a Breach

- Assessment of Applicable Laws
- Understand Government and Trade Standards
- Have Good Protocols
- Assess Compliance

FEDERAL TRADE COMMISSION
FOR THE CONSUMER

- Take Stock
- Scale Down
- Lock It
- Pitch It
- Plan Ahead



FEDERAL TRADE COMMISSION
FOR THE CONSUMER

Enforcement

- GLBA
- FCRA
- FTC ACT – Section 5
  - Deceptive Practices
  - Unfair Practices

SO WHAT NOW?

- "It is important to note, however, that there is no such thing as perfect security and breaches can happen even when a company has taken every reasonable precaution."

  Deborah Platt Majoras, Prepared Statement of the Federal Trade Commission before the United States Senate Committee on Commerce, Science, and Transportation, June 16, 2005, p. 6.

- STANDARD - KNOW UNREASONABLE WHEN SEE IT

- SOME GUIDANCE
  - Consent Decrees
  - GLBA Safeguard Provisions
  - Private Standards

- Inadvertently Disclosed 669 Prozac Mailing List Subscribers
- Violated Privacy Statement
- Consumer Deception
- Consent Decree – Develop Security Program

OTHER DECEPTION CASES

TOWER RECORDS
Tower.com

Microsoft
Your potential. Our passion.™

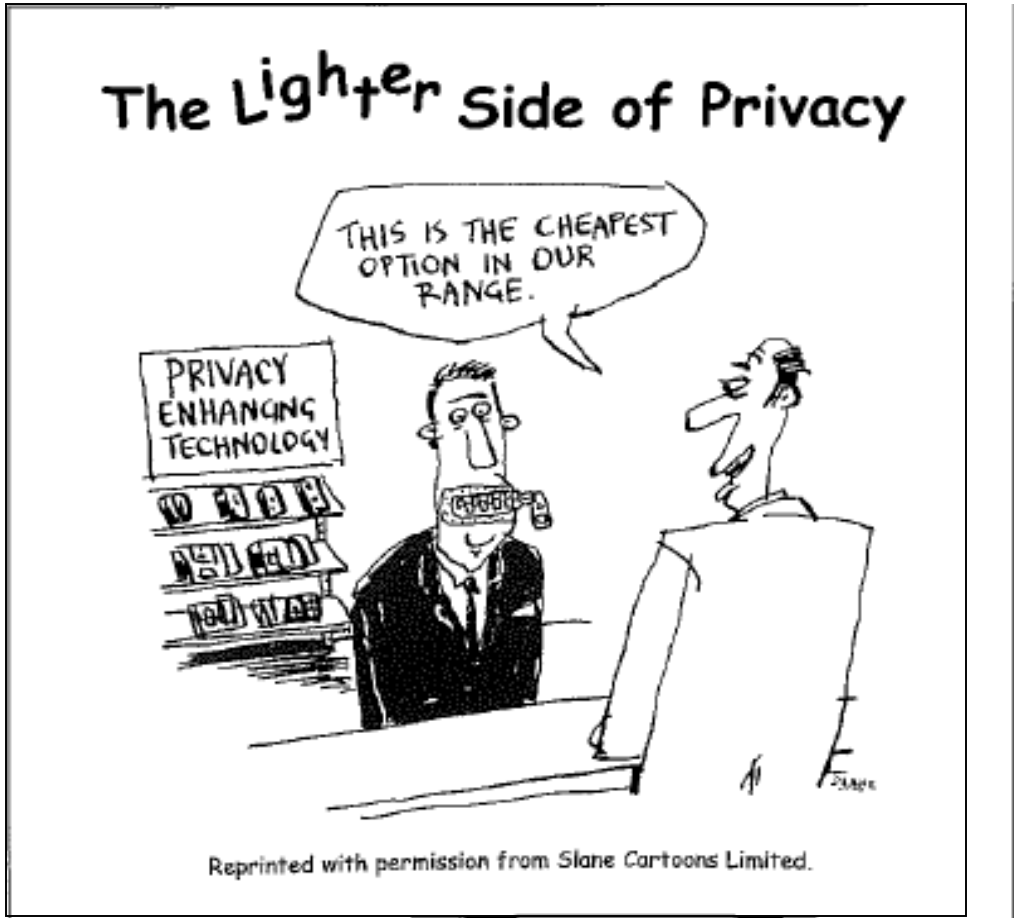
PETCO
Where the pets go.

GUESS®
U.S.A.
WASHED
JEANS

Life is good.®

Consent Decrees

- Data Encryption
- Perimeter Security
- User Screening
- Learning Mechanism
- Foreseeable Risks
- User Authentication



BJ's WHOLESALE CLUB®
Where values come to life.®

- B.J's made no assurances of a certain level of data protection when collecting customer data
- FTC looked to B.J.'s security procedures and practices, deemed them to be insufficient
- Charged B.J.'s with engaging in conduct unfair to consumers
- **FTC signaled to companies that it was making the protection of consumer privacy rights a top priority for the agency**

BJ's WHOLESALE CLUB®
Where values come to life.®

- Failed to safeguard customer information from debit or credit cards
- Failed to encrypt information
- Stored information in files that could be accessed anonymously
- Kept information longer than necessary

TRUSTED WISDOM. EXTRAORDINARY RESULTS.

DSW

- Over 100,000 consumers notified
- Retained information in multiple files
- Stored unencrypted
- Could be accessed with commonly known user ID and password
- Failed to limit wireless connection to information

ChoicePoint

- 145,000 consumer's personal information
- Compromised after identity thieves established ChoicePoint accounts
- FTC investigated privacy, verification, and compliance practices
- Found ChoicePoint failed to monitor or identify unauthorized activity (despite notification from law enforcement)
- Made misleading representations regarding safeguards

ChoicePoint

- Comprehensive Security Program with Third Party Audit for 20 years
- $5 Million into Fund for Potential Consumer Redress
- $10 Million Fine for Violations of FCRA

Largest Fine Ever Levied by the FTC

seisint™

- 316,000 Consumers in March 2005
- Complaint Concerned User Credentials
  - Easy to Guess Credentials
  - Sharing of Credentials
  - Periodic changes of Credentials
  - Suspend Credentials After Unsuccessful Attempts
  - Credentials in Cookies
  - Encryption in transit
  - Monitoring of Credential Creation
- Comprehensive Security Program with Third Party Audit for 20 years

LexisNexis™

- PIN Entry Device Skimming
- Closing Letter

"[1] the nature and magnitude of the risk relative to other risks;

[2] the benefits relative to the costs of protecting against the risk;

[3] Dollar Tree's overall data security practices;

[4] the duration and scope of the compromise;

[5] the level of consumer injury; and

[6] Dollar Tree's prompt response."

GLBA Safeguard Provisions

- Designation of an employee to manage safeguards
- Review of risk management of each department
- Plan for developing, monitoring, and testing a program to secure information
- Plan for changing safeguards as needed

Identity Theft Red Flag Rules

- Financial Institution and Credit
- Opening Accounts and Existing Accounts
- Guidelines to detect, prevent, and mitigate Identity Theft
  - –Verify Identity
  - –Proactive
  - –Training
  - –Oversee Service Provider
  - –Involve Board and Senior Management
- Effective November 2008

Regulation S-P

Safeguard Information and Response to Security Breach

- Securities Industry (broker, dealer, investment company, adviser or transfer agent)
  - Service Providers
- Comprehensive Security Program
  - Ensure security against reasonably foreseeable treats
  - Designate Employee
  - Test and Otherwise Monitor
  - Oversee Service Providers
- Notification in Event of Breach if misuse "reasonably possible"

TRUSTED WISDOM. EXTRAORDINARY RESULTS.

PCI DSS

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Preparing for a Breach

- Assessment of Applicable Laws
- Understand Government and Trade Standards
- Have Good Protocols
- Assess Compliance

TRUSTED WISDOM. EXTRAORDINARY RESULTS.

Breaches and Consumer Notices – The Importance of Having a Plan and What to Include in a Plan

Have a Plan

- DEVELOP/IMPLEMENT/MAINTAIN COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM
  - Administrative, technical, and physical safeguards
  - Designed to ensure security and confidentiality
- DESIGNATE EMPLOYEE(S) TO COORDINATE
- IDENTIFY POINTS OF RISK
- DESIGN/IMPLEMENT SAFEGUARDS TO CONTROL RISKS AND REGULARLY TEST AND MONITOR

Follow the Plan

- ASSESS RISKS:
  - Employee training and management
  - Information systems
  - Detecting/preventing/responding to attacks against institution's systems
- ASSESS SUFFICIENCY OF SAFEGUARDS IN PLACE TO CONTROL THE RISKS
- REGULARLY TEST AND MONITOR SAFEGUARDS
- OVERSEE SERVICE PROVIDERS, INCLUDING CONTRACTORS
  - Contractors must be capable of, and be required by contract to, maintain and implement appropriate safeguards

Questions?

Oscar Marquis
Oldaker, Biden & Belair, LLP

818 Connecticut Ave NW, Suite 1100
Washington, DC 20006

omarquis@obblaw.com
(202) 728-1010
Direct Dial: (847) 698-1077
Fax: (847) 692-9469

Ronald I. Raether, Jr.
Faruki Ireland & Cox P.L.L.

500 Courthouse Plaza
10 North Ludlow Street
Dayton, Ohio 45402

rraether@ficlaw.com
Direct Dial: (937) 227-3733
Fax: (937) 227-3717