



### Information

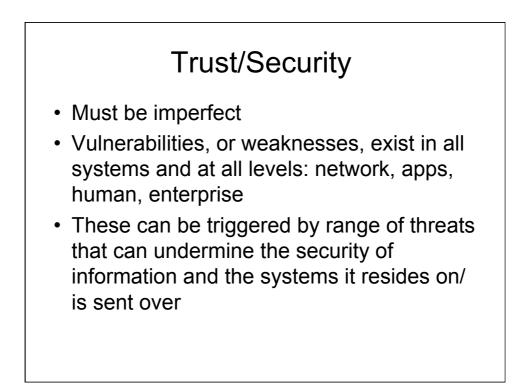
- · Personal data of value to others
  - Banking, education, credit history, medical records,
  - What you buy/pay for
  - What you watch/read/listen to/play online
  - What online services you use, subscribe to
  - Where you are: location data
  - Who you call, text, email

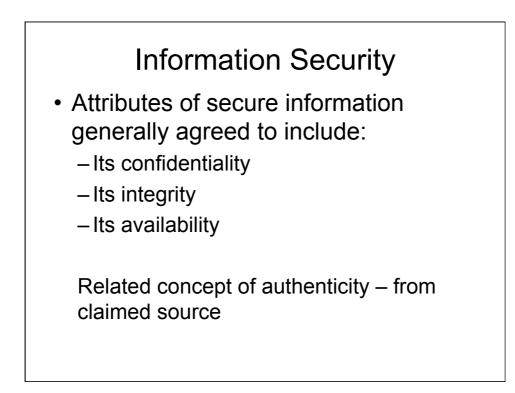
### ICT Dependency Many sectors important to the functioning of

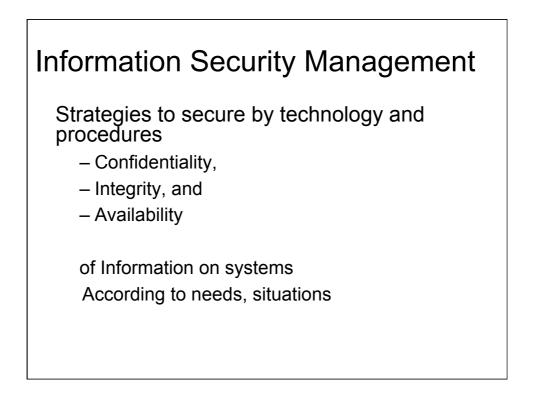
- Many sectors important to the functioning of society use ICT to operate, including to run the controls or provide the physical architecture for many things:
  - financial markets,
  - money transfers,
  - transport systems,
  - emergency services,
  - health services,
  - power and water supply, business supply chains, etc.

# ICT Dependency

- Often such critical sectors are interconnected: eg, energy sector powers communications towers and transport systems
- Great concerns about security of critical infrastructure and the need for 'circles of trust'
  - Trust is not binary
    - Rather relative reflecting history, nature/value of information, relationship, knowledge, skills, etc., level of security





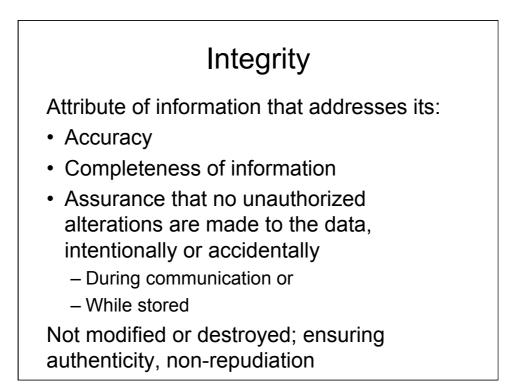


# Confidentiality

Controlling the disclosure of information (1) protecting it/systems so that unauthorized persons cannot have access to it, and/or

(2) protecting information so that even if unauthorized access is obtained, information is unreadable (e.g. encrypted).

- · Authenticating identity of seeker of access
- · Access only to authorized level



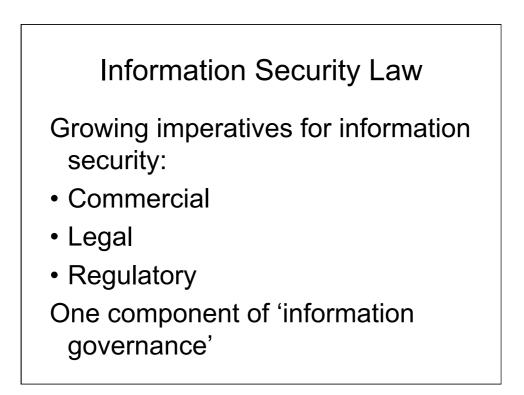
# Availability

Involves ensuring that computer systems, networks, and data on/over them are:

- operational,
- fully functioning,
- available for use, and
- accessible whenever need

Timely and reliable access to and use of information

Issues: Withstand disruptions; address technological obsolescence and media deterioration



# The imperatives for information security

- Commercial
  - Trustworthiness of business transactions
  - -Growing risk
  - Economic and legal consequences
    - Value, importance of information of various kinds
  - -Marketing/image

# Drivers of Information Security

- Legal
  - Growing legal frameworks addressing information security issues/obligations/liability prompted by concerns regarding cybercrime, privacy, safety of critical infrastructure and economic security
- Regulatory
  - Enforcement at various levels as a response to ineffective self-regulation

# **IS Legal Trends**

1. Expanding legal duties, including general duties, to provide appropriate information security for an organization's data and electronic transactions;

- 2. Legal standards for what is 'reasonable' security emerging;
- 3. Legal duties to warn those affected (stakeholders) affected by security breaches
  - US states, EU Framework Directive (PECN), GDPR



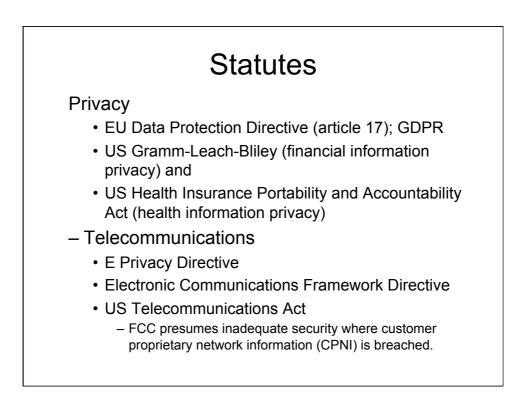


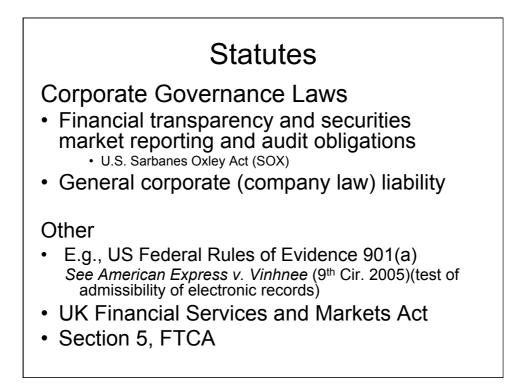
# Characteristics of legal duties to protect information

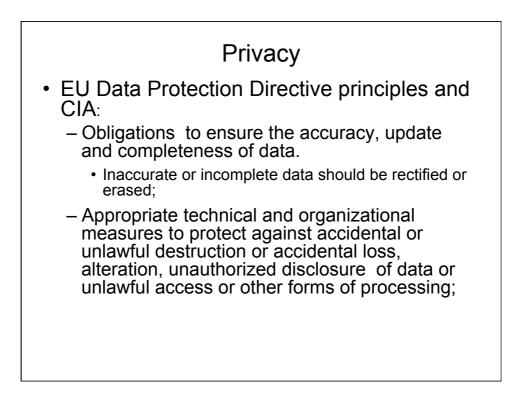
- Evolving and expanding
- Global impact
  - US, EU, OECD (soft law), etc.
- · Growing scope:
  - Kinds of information
  - Who is target of protection; of duty
- Variety of sources
  - Patchwork with possibility for multiple obligations

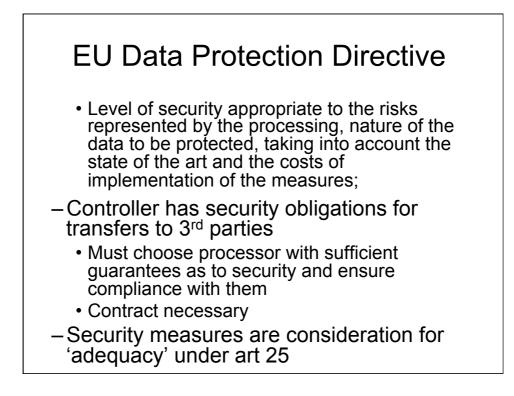
### Sources of Obligations

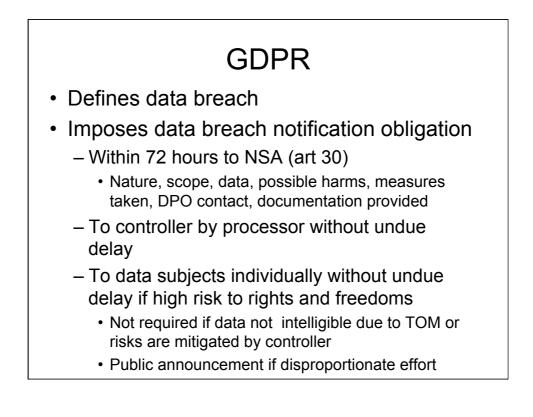
- Statutes
- Regulations
- Private law
  - Business partner obligations (contract)
  - Victims (tort)
- Common Law
  - Evidentiary Rules





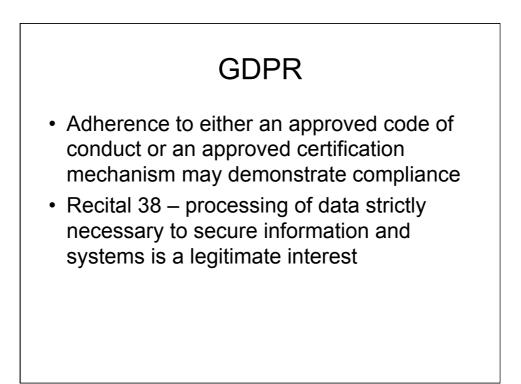


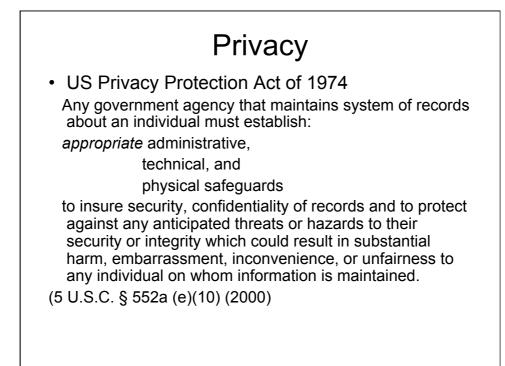


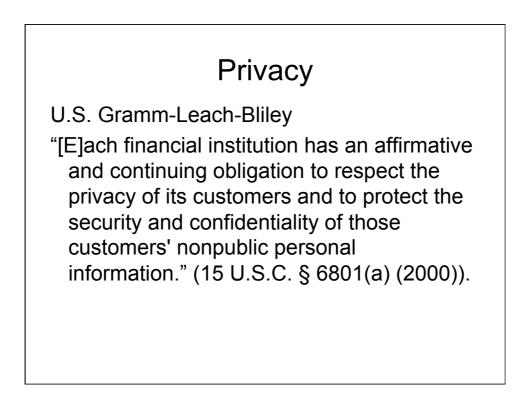


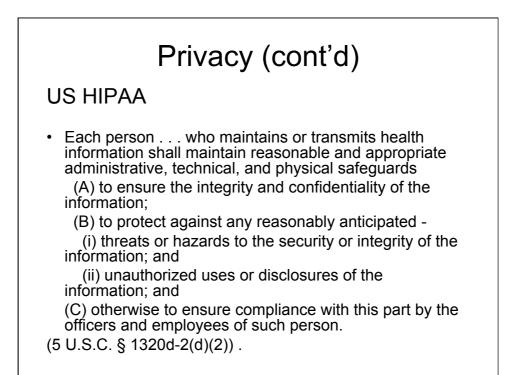
# GDPR

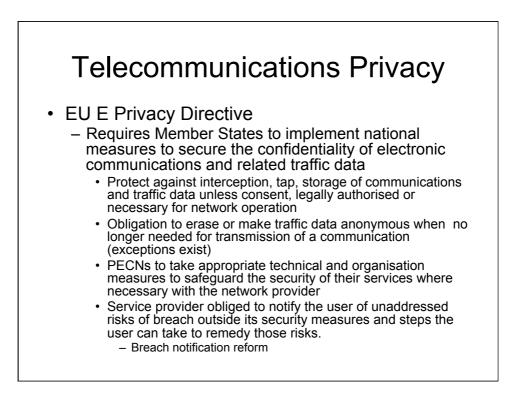
- Specific suggestions for security actions m "appropriate to the risk," including:
  - Pseudonymisation. and encryption
  - Ability to ensure the ongoing CIA and resilience of systems and services
  - Ability to restore availability and access to data in a timely manner in event of physical or technical incident.
  - Process for regularly testing, assessing and evaluating the effectiveness of TOM.

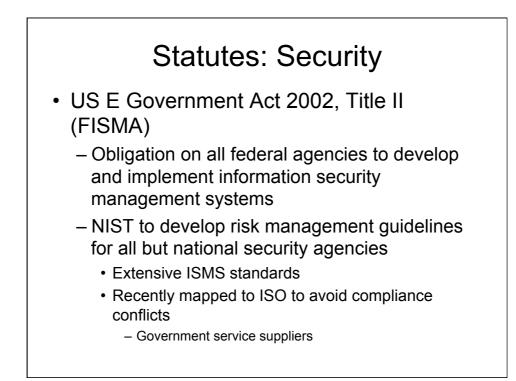


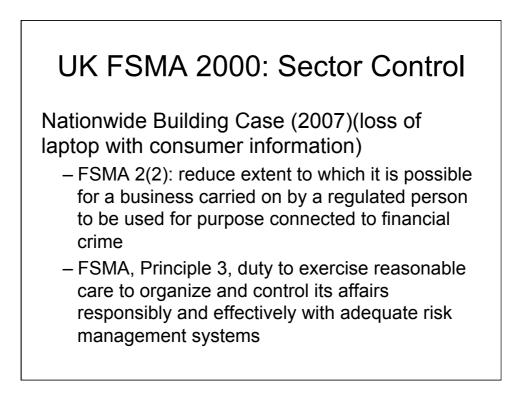








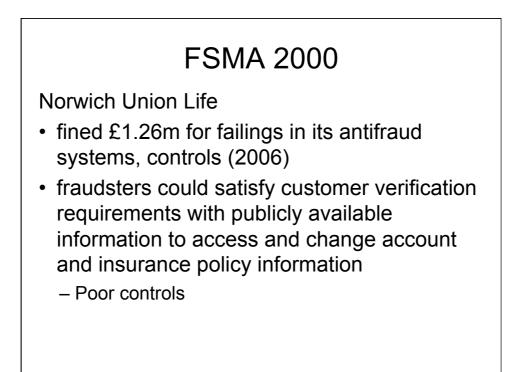




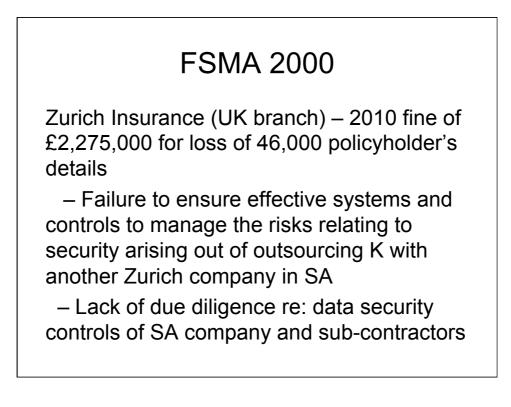
## Nationwide Bank

- Inadequate controls
- Different locations
- Inconsistent policies
  - Lacked prioritization
  - Clarity
- · Generic training with limited oversight
- Poor incident management procedures

   Further ability to use for financial crime

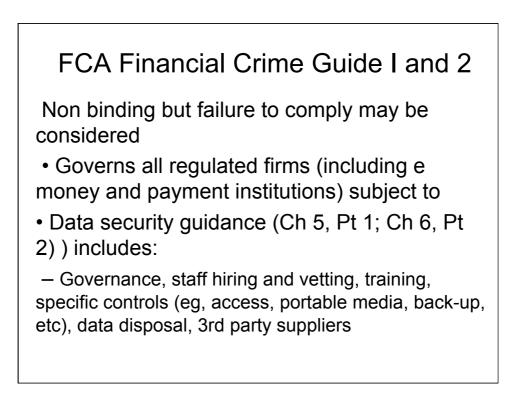


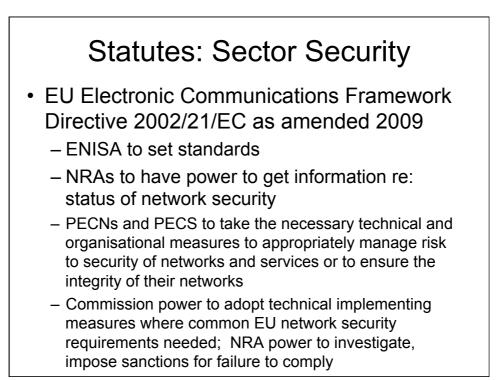
# Norwich Union Failure to respond timely by management even though compliance department identified £3.3 million policies surrendered in one year (74policies) Unclear policies as to who was responsible for response management Failure to give adequate risk balancing with customer service

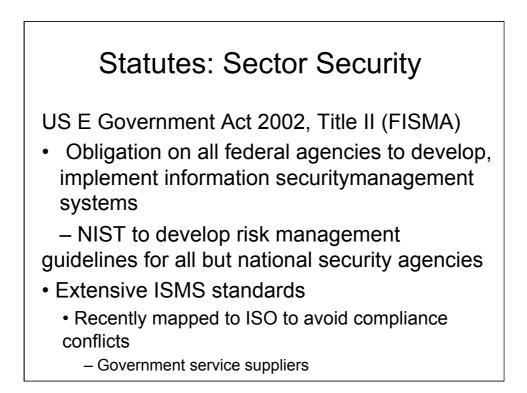


# Zurich Insurance

- Reliance on group policies w/o considering whether comprised adequate security, whether in place
- · Failure to identify adequately lines of
- responsibility- many people task with IS duties but no one with overall responsibility
- Poor system controls in failing to discover that unencrypted back up tape with details missing for over a year







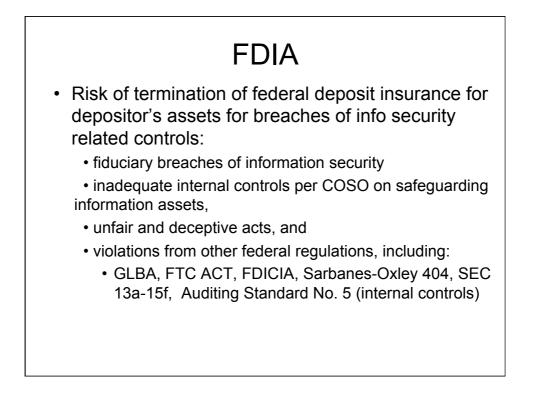
# Sector Obligations: US FDIA

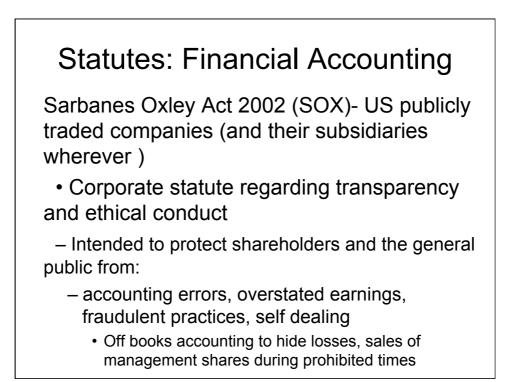
Law providing federal deposit insurance to financial institution customers

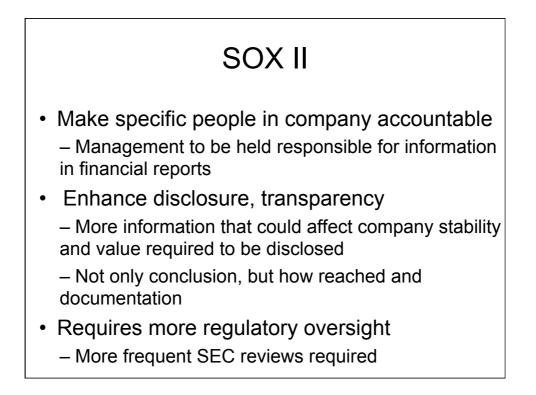
- Under Sec 39 –safety and system controls
  - Unsafe or unsound practice standard

• Directors of 16,000 federally insured banks, savings institutions and credit unions are legally obligated to safeguard information assets including from identity theft.

 Interagency guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect CIA







# SOX III

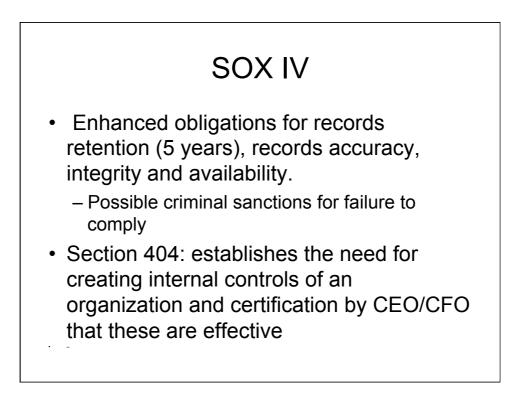
• Increased financial reporting obligations to ensure greater transparency for investors

 Reporting of significant events that can affect value of company (e.g. change in management)

Various time limits (e.g., 4 days)

Sign-off by executive management that reports are accurate

Criminal sanctions



# SOX V

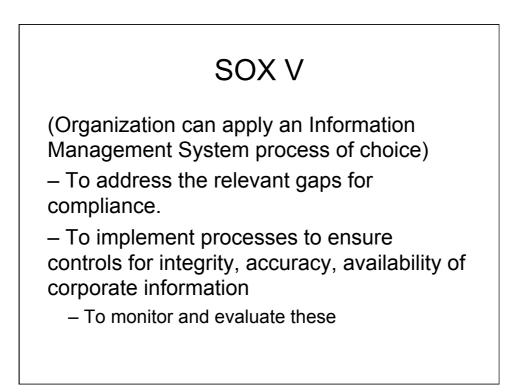
Each public company must develop individual approach to compliance and reporting.

• Self-assessment of the internal controls the organization has for its financial reporting process.

- Internal and external audit teams

 Evaluate under some standardized framework (e.g. COSO) to identify the gaps in compliance, as well as any associated risks.

• Allows audit firms to map internal control objectives back to SOX requirements,



# SOX and ISM

Indirect but significant impact of law

 CEO cannot sign off on accuracy of financial
 information if possibility that based on corrupted,

invalid or incomplete data – CEO cannot sign off that has internal controls in place if systems that run these are not up and

secure
Cannot meet specific records provisions if not

secure systems and information

UK Companies (Audit, Investigations and Community Enterprise) Act of 2004

Directors must issue a statement in auditor's report, confirming that they provided the auditors with all of the relevant information needed to properly prepare the report.

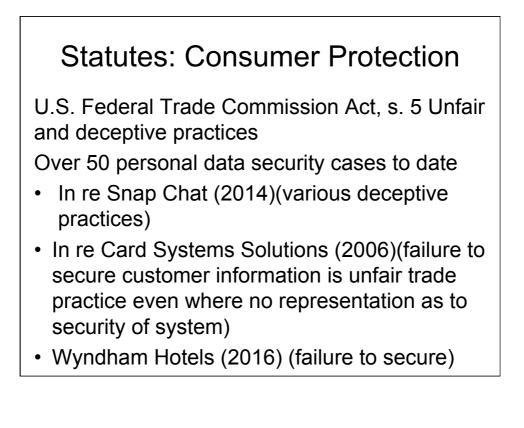
 Directors who fraudulently or negligently make statement – or who fraudulently or negligently allow the statement in the report – commit an offence punishable by fine or imprisonment.
 Likely commensurate impact on IS

# SEC: Corporate Disclosure Investor Transparency Reporting under Securities and Exchange Act of 1934

 2010 guidance issued re: material risks concerning information security and intrusions of concern to reasonable investor

• Eg. whether caused a loss of intellectual property, sparked lawsuits against the company, damaged its sales, harmed its customers or suppliers or prompted it to "materially increase its cybersecurity protection expenditures.

• Other cyber risks including the "consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption".



# Statutes: US Breach Notification

# Regulations Records retention obligations in laws US Internal Revenue Service regulations requiring security for electronic tax records Consumer Protection U.S. Federal Trade Commission Act In re CardSystems Solutions, Inc., FTC File No. 052 3148 (Feb. 23, 2006)(failure to secure customer information is unfair trade practice even where no representation as to security of its system.) But see, Wyndham Hotels countersuit Victim, FTC lacks exertise and authority to address IS under 'unfair' and 'deceptive'; no standards

# Discussion re: Amex v. Vinhee