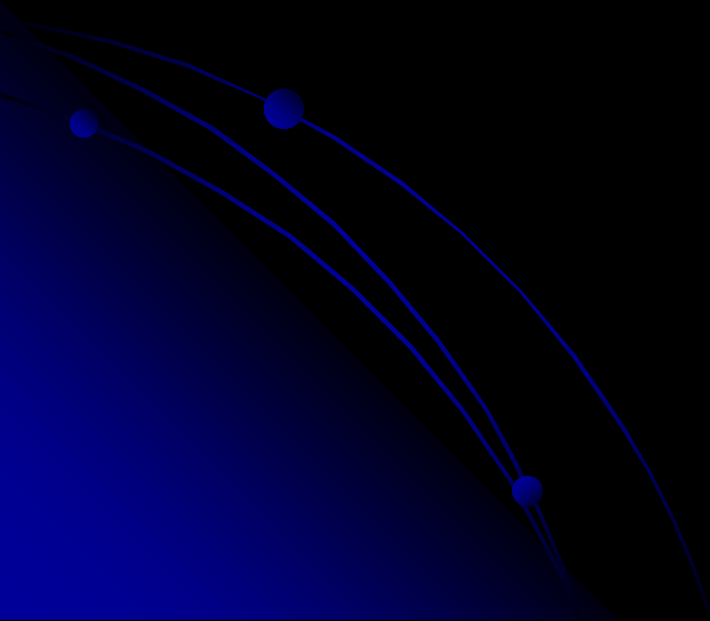


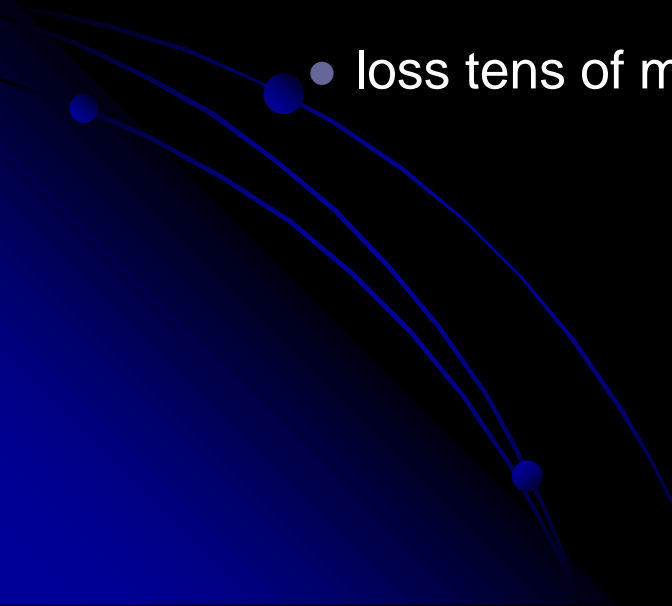
THE EVOLVING ZONES OF PRIVACY: SAFEGUARDING THIRD PARTY INFORMATION AND MINIMIZING PRIVACY CLAIM EXPOSURE

Presented By

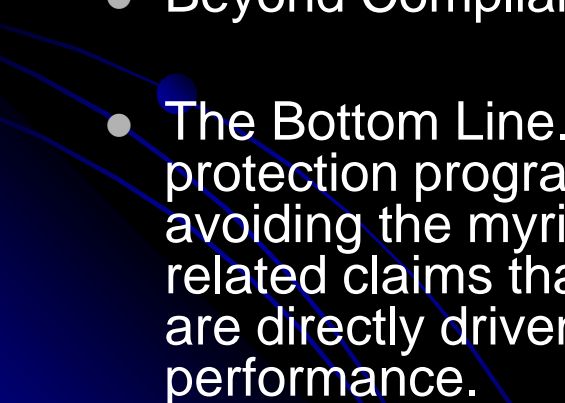
LAURA J. COE



INTRODUCTION

- Why Privacy Law Issues Matter
 - During 2017, over 1,500 data breaches resulted in:
 - disclosure of the sensitive personal information in more than 170M records; and
 - loss tens of millions of dollars in the form of identity theft.
- 

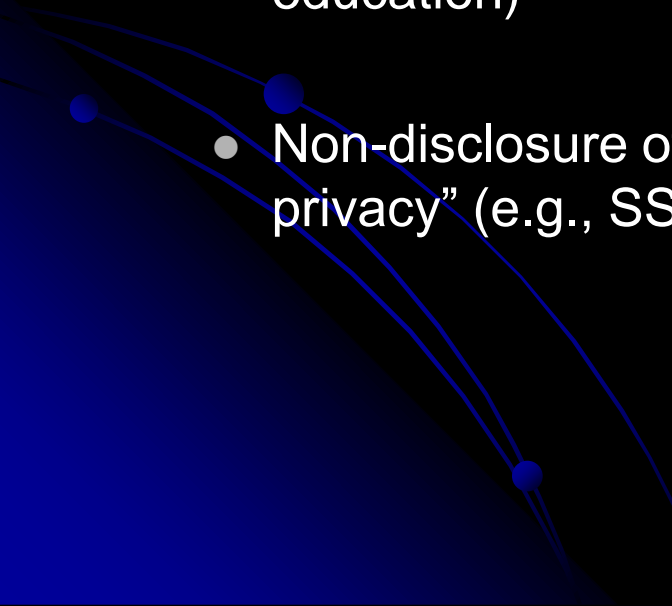
INTRODUCTION

- Why Your Business Should Be Concerned About Privacy and Data Protection
 - Compliance Issues. Many businesses are required to comply with federal and/or state laws requiring businesses to safeguard non-public personal information or face stiff fines and penalties (ranging from tens of thousands to millions of dollars).
 - Beyond Compliance. Lose trust and you lose your client.
 - The Bottom Line. A well-designed and well-run privacy data and protection program improves a company's bottom line by avoiding the myriad of costs associated with data breaches and related claims that may arise. Recent data also suggest sales are directly driven by business' privacy reputation and performance.
- 

INTRODUCTION

- Brief History of Privacy Law
 - Impact of Digital/Information Age on Privacy
 - Statutory Framework
 - The GLBA
 - Texas Identity Theft Enforcement and Protection Act
 - Potential Common Law Liability
 - What You Can Do to Protect Your Business
- 

BRIEF HISTORY OF PRIVACY LAWS

- Individual Privacy Interests Protected Under the United States Constitution
 - Independent decision making regarding matters within the “zones of privacy” (e.g., matters related to marriage, procreation, contraception, family relationships, and child rearing and education)
 - Non-disclosure of personal matters outside the “zones of privacy” (e.g., SSN, DLN, DOB)
- 

BRIEF HISTORY OF PRIVACY LAWS

- Privacy Laws from Cradle to the New Millennium
 - Basic Concepts of the Right to Privacy: Zones of Privacy
 - *Griswold v. Connecticut* (1965)
 - U.S. Supreme Court determined the right to privacy is a fundamental right
 - Privacy is implicit in the 1st, 3rd, 4th, and 5th Amendments
 - Non-Disclosure of Personal Matters Outside the Zones of Privacy
 - During most of the nearly 40 years following *Griswold* not much concern was paid to matters outside the zones of privacy.

THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

- Data Breaches

- The Statistics. The following statistics reflect data breaches identified by the Identity Theft Resource Center for 2017

INDUSTRY	# OF BREACHES	# OF RECORDS IMPACTED
Banking/Credit/Financial	134	3,122,090
Business	870	163,449,242
Educational	127	1,418,258
Government/Military	74	5,903,448
Medical/Healthcare	374	5,062,031
Total for all Industries	1,579	178,955,069

THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

- The Businesses. The following are just a few examples of data breaches identified by the Identity Impacted Theft Resource Center for 2007 (through October 9, 2007):

BUSINESS	RECORDS EXPOSED
Merrill Lynch	33,000
Chase/Bank One	4,100
JP Morgan Chase	47,000
Bank of America	Unknown #
Venetian Casino Resort	Unknown #
Gap, Inc.	800,000
Life Time Fitness	100
American Airlines	350
Neiman Marcus Group	160,000
Texas A&M	8,049
American Ex-POWs	35,000
Texas Secretary of State Web	Unknown #
FEMA	2,300
CVS Corporation	1,000
John Hopkins Hospital	52,000

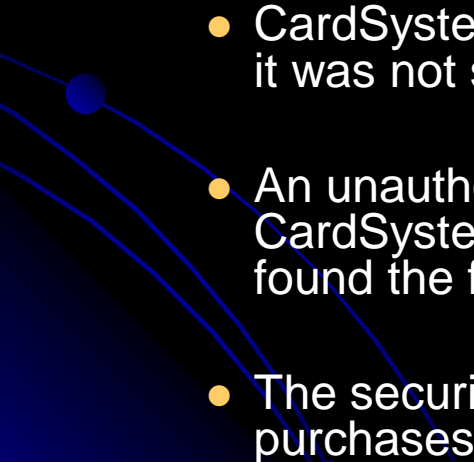
THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

- Lawsuits/Enforcement Actions
 - Life Time Fitness, Inc. (aka the Dumpster Bust)
 - Case Facts
 - Texas Attorney General sued Life Time Fitness, Inc. (LTF) for failing to safeguard its customers' personal data.
 - The lawsuit alleges that during April through June 2007, more than 100 business records containing sensitive customer information (e.g., dates of birth, credit card numbers, Social Security numbers, and, in some instances, photocopies of driver's licenses and Social Security cards, as well as other information) were found in trash bins adjacent to LTF locations in the DFW metroplex.
 - The lawsuit alleges that LTF's improper disposal of these records constitutes violations of the DTPA and Identity Theft Enforcement and Protection Act.

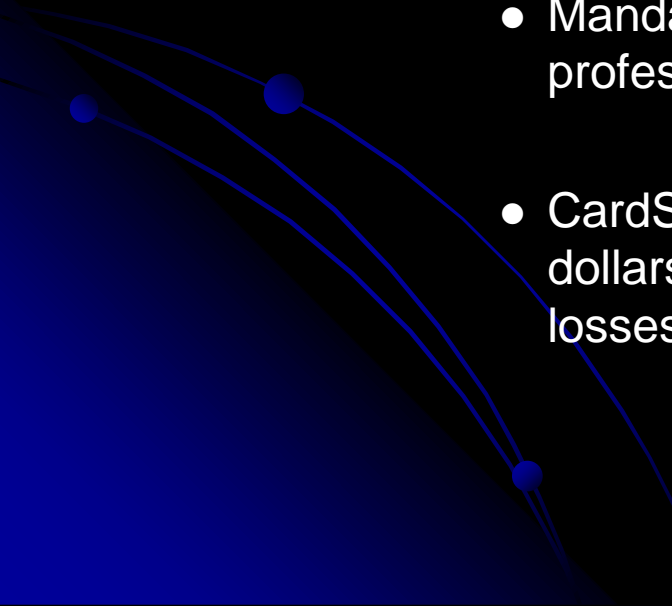
THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

- Potential Exposure
 - The lawsuit is seeking:
 - civil penalties of up to \$500 for each business record that was not properly disposed of (i.e. $\$500 \times 100 = \$50,000$);
 - up to \$50,000 for each violation of the Identity Theft Enforcement and Protection Act (i.e. $\$50,000 \times 90 = \$4,500,000$); and
 - other penalties (e.g., unknown potential exemplary damages).

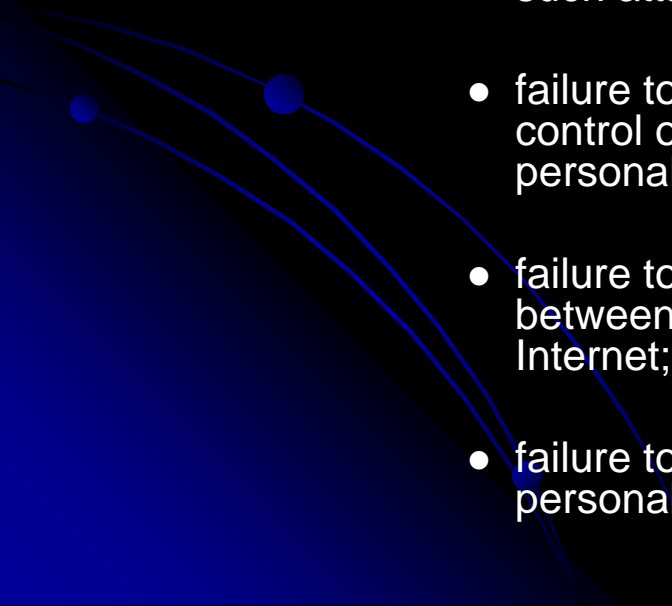
THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

- CardSystems Solutions, Inc. (aka the MasterCard-Visa Heist)
 - Case Facts
 - MasterCard-Visa allowed 40 million customer credit card numbers to be sucked out of their systems and into the hands of criminals in what is the largest known compromise of financial data to date.
 - CardSystems, the third party service provider, put information it was not supposed to keep into the wrong file.
 - An unauthorized third party was able to get behind CardSystems' firewall, insert a code into the system that found the file, and download the data to her own system.
 - The security breach resulted in millions of dollars in fraudulent purchases causing the FTC to institute an enforcement action.
- 

THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

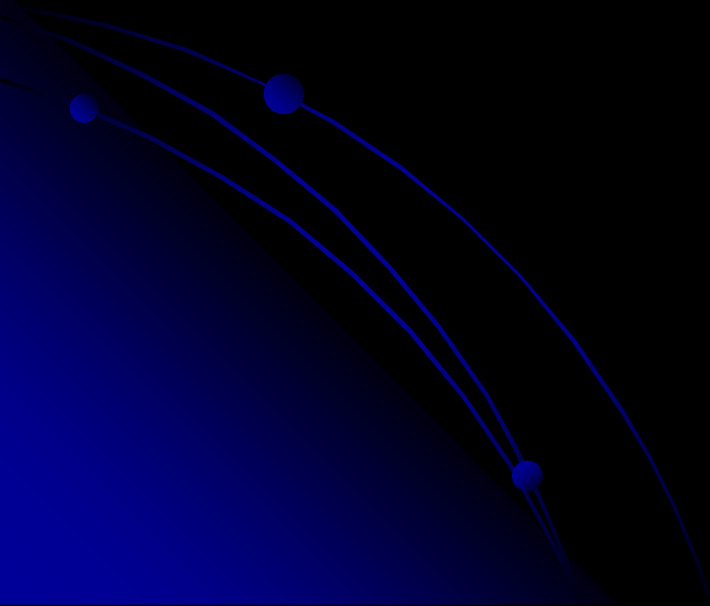
- The Outcome
 - The FTC settled with CardSystems under the following terms:
 - Implementation of a comprehensive information security program;
 - Mandatory audits by an independent third party security professional every other year for 20 years; and
 - CardSystems faces potential liability in the millions of dollars under bank procedures and in private litigation for losses related to the breach.
- 

THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

- Practices that, taken together, may constitute negligence in the security of sensitive consumer information:
 - creation of unnecessary risks to customer information by storing it;
 - failure to adequately assess the vulnerability of your computer network to commonly known or reasonably foreseeable attacks (e.g., "Structured Query Language" injection attacks);
 - failure to implement simple, low-cost, and readily available defenses to such attacks;
 - failure to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network;
 - failure to use readily available security measures to limit access between computers on its network and between its computers and the Internet; and
 - failure to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.
- 

THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

- Lessons from CardSystems
 - Do not maintain information that you have no reason to keep.
 - If you do, do not store the information in a way that puts consumers' financial information at risk.

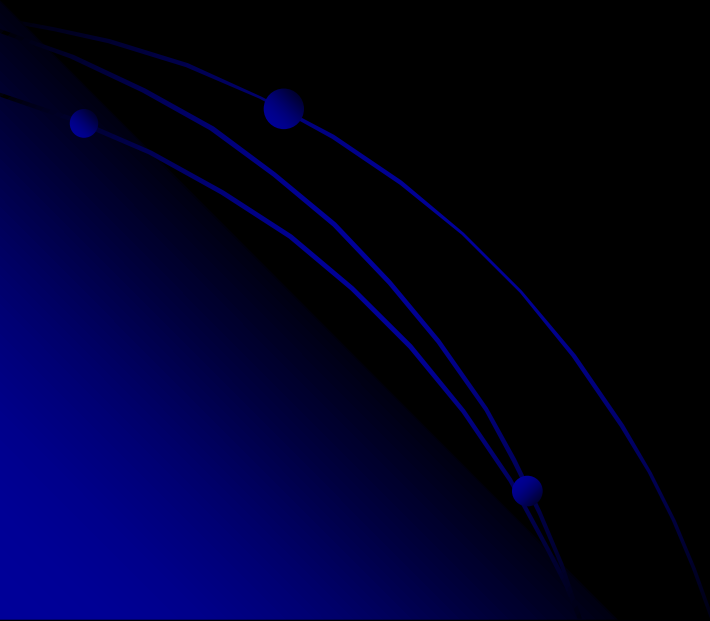


THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

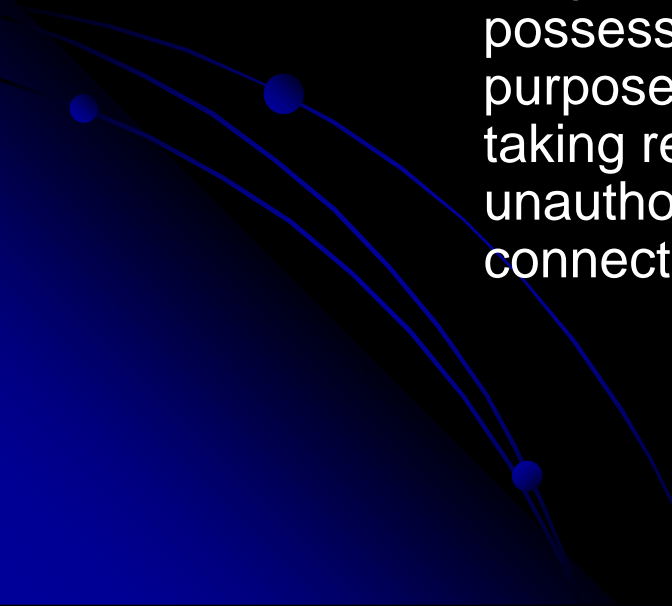
- ChoicePoint, Inc.
 - Case Facts
 - ChoicePoint, Inc. (CP), a national provider of identification and credential verification services, maintains personal profiles of nearly every U.S. consumer, which it sells to employers, landlords, marketing companies and about 35 U.S. government agencies.
 - The incident was not the result of its systems being hacked but rather caused by criminals posing as legitimate businesses seeking to gain access to personal information.
 - The criminals gained access to more than 160,000 people's names, addresses, Social Security numbers and credit reports. 800 people reported identity theft issues, causing the FTC to institute an enforcement action.

THE RIGHT TO PRIVACY IN THE TWENTY FIRST CENTURY: THE IMPACT OF THE DIGITAL/INFORMATION AGE ON PRIVACY

- The Outcome
 - CP settled with the FTC for \$10 million in civil penalties and \$5 million for consumer redress expenses.

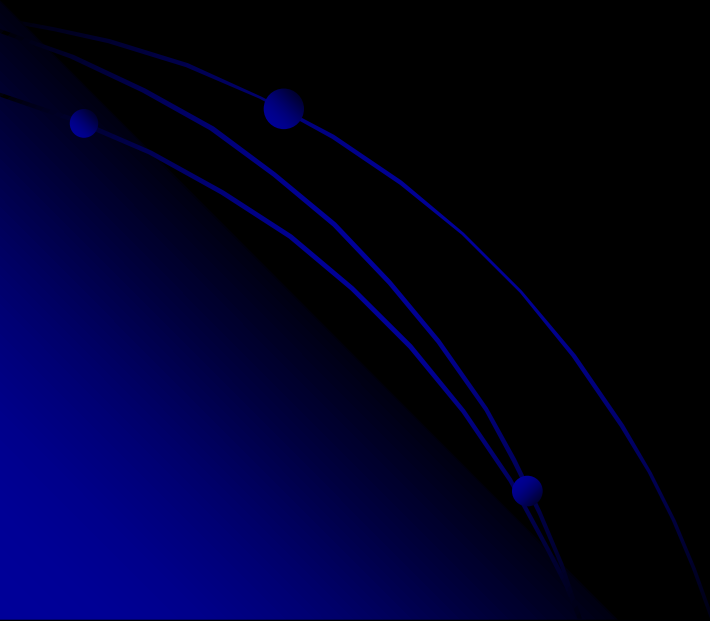


THE PRIVACY LAW STATUTORY FRAMEWORK

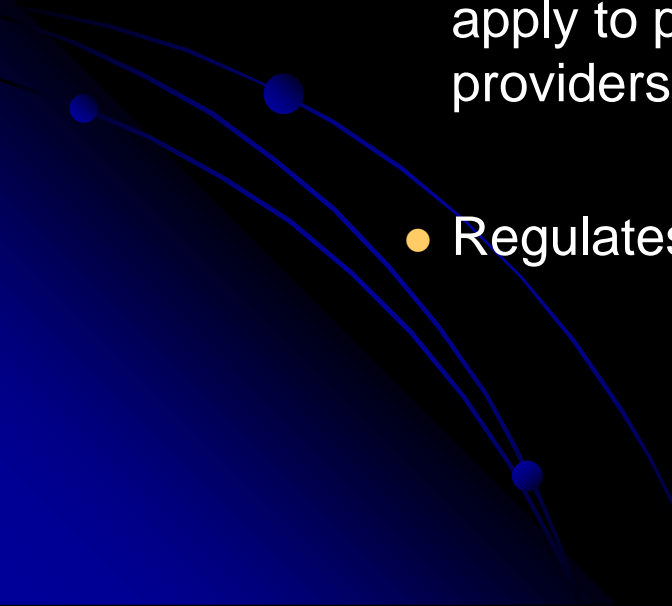
- Federal Law
 - Significant Federal Privacy Laws Applying to Businesses
 - The Fair and Accurate Credit Transactions ("FACT Act") (Disposal Rule)
 - Requires that any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.
- 

THE PRIVACY LAW STATUTORY FRAMEWORK

- The Gramm-Leach-Bliley Act ("GLBA")
 - Imposes data security requirements on a wide range of financial and related firms holding customer data.

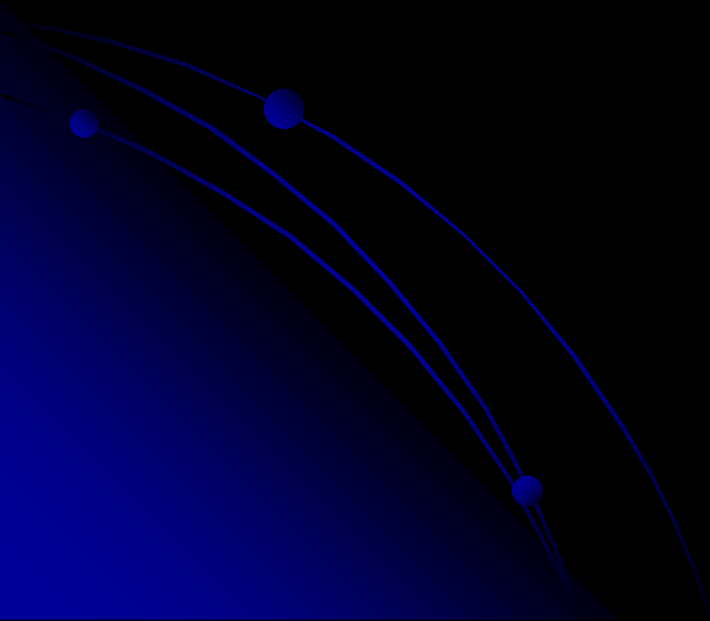


THE PRIVACY LAW STATUTORY FRAMEWORK

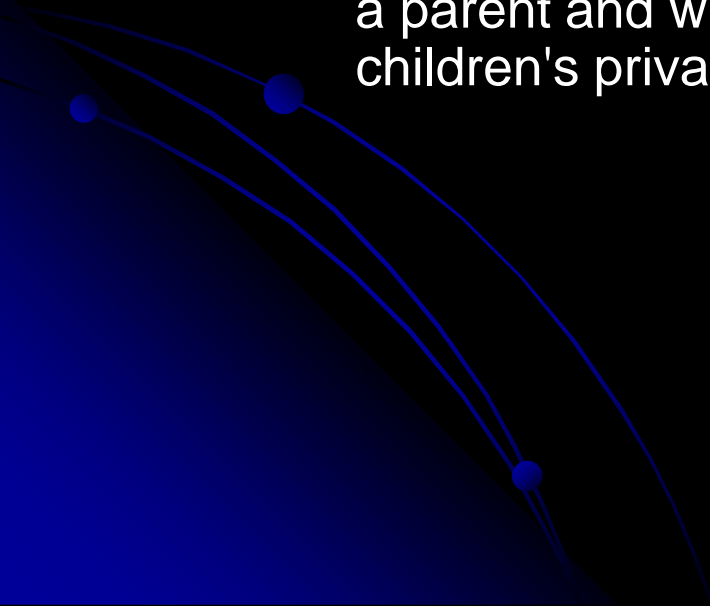
- The Privacy Act
 - Establishes eleven Information Privacy Principles (IPPs) which apply to Commonwealth and certain government agencies.
 - Includes ten National Privacy Principles (NPPs) which apply to parts of the private sector and all health service providers.
 - Regulates credit providers and credit reporting agencies.
- 

THE PRIVACY LAW STATUTORY FRAMEWORK

- Specialized Legislation to Keep in Mind
 - Americans with Disabilities Act ("ADA")
 - Prohibits employers from disclosing medical information about applicants and employees.

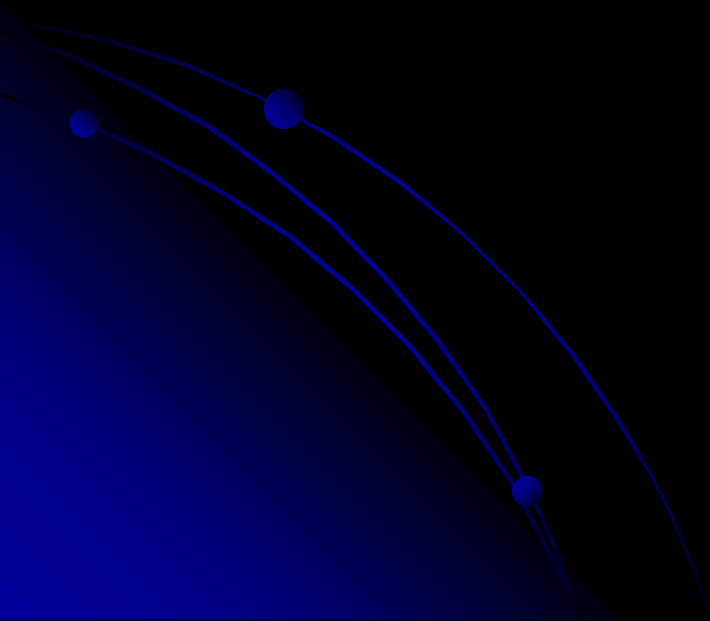


THE PRIVACY LAW STATUTORY FRAMEWORK

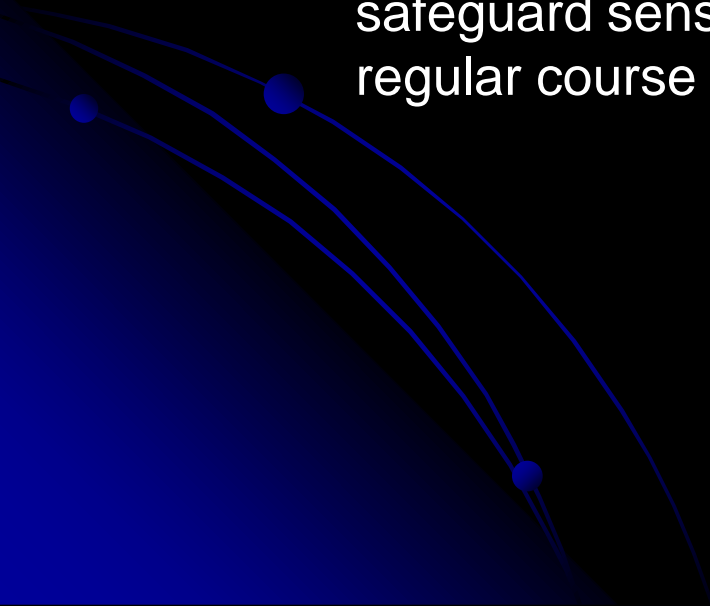
- Children's Online Privacy Protection Act ("COPPA").
 - Applies to the online collection of personal information from children under 13.
 - Establishes what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.
- 

THE PRIVACY LAW STATUTORY FRAMEWORK

- Health Insurance Portability and Accountability Act ("HIPAA")
 - Establishes protection for the privacy of personal health information.



THE PRIVACY LAW STATUTORY FRAMEWORK

- Texas Law
 - The Texas Identity Theft Enforcement and Protection Act
 - Provides for enforcement actions by the Texas Attorney General, including the imposition of fines and penalties for failure to implement and maintain reasonable procedures to safeguard sensitive personal information collected in the regular course of business.
- 

THE PRIVACY LAW STATUTORY FRAMEWORK

- Other Jurisdictions
 - Life Outside the Republic
 - Texas businesses engaging in transactions with individuals in other states and/or countries may also be subject to the privacy laws of those jurisdictions.
- 

THE PRIVACY LAW STATUTORY FRAMEWORK

- California
 - Security Breach Information Act
 - Punishes negligent disclosure by creating a clear duty to protect personal information.
 - Mandates notice to consumers of a breach in the security, confidentiality, or integrity of unencrypted computerized personal information held by a business or government agency.
 - Provides for a civil cause of action to recover damages by any person damaged as a result of a violation of the Act.

THE PRIVACY LAW STATUTORY FRAMEWORK

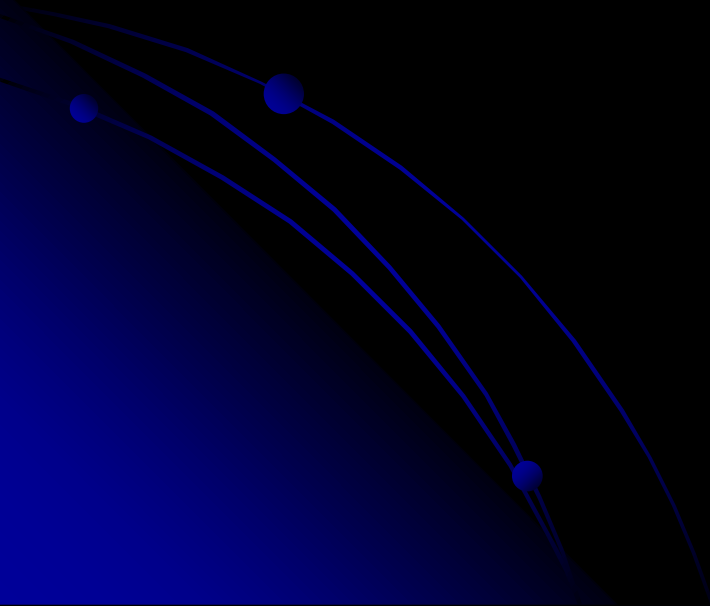
- Other States' Laws
 - A majority of states that have adopted security breach laws have created a duty to disclose breaches.
 - Few have adopted a civil cause of action for individuals harmed, and fewer apply the laws to such a broad category of entities as California.
 - New York (and Texas), for example, enacted notice statutes but limit the enforceability to an action brought by the state Attorney General's office.
 - Other states limit the application to government entities, data brokers, non-financial institutions, non-HIPAA entities, or any combination of the mentioned groups.

THE PRIVACY LAW STATUTORY FRAMEWORK

- States As Leaders on Privacy Protection
 - By the end of 2005, at least 39 states had enacted security breach notification laws. At least nine of these laws have no harm trigger.
 - Thirty-nine states have enacted security freeze legislation.
 - As many as forty states had already enacted "do not call lists" before the FTC acted in 2003 to establish a national list.
 - Two states--Washington and California--granted consumers the right to obtain business records from firms where identity thieves used their names, before Congress added this benefit in the FACT Act.
 - Over a dozen states had enacted laws requiring the truncation of credit card numbers on consumer receipts before the provision was made nationwide in the FACT Act.

THE PRIVACY LAW STATUTORY FRAMEWORK

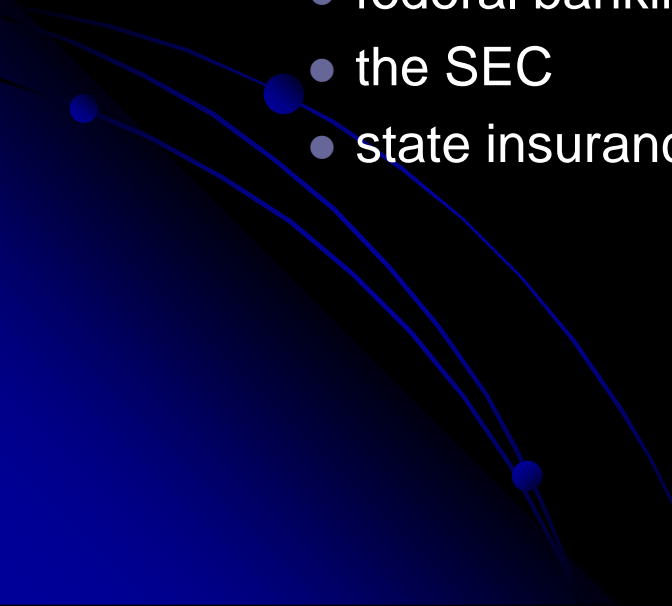
- A Word on Preemption
 - A marketplace where a consumer can buy products from only one seller is not competitive, nor is a public policy marketplace of ideas which is restricted to Congress.
 - No existing decisions regarding pre-emption of state privacy statutes outside of the HIPPA context.



THE GLBA

- Who Is Subject to the Act
 - "Financial institutions" significantly engaged in such financial activities.
 - "Financial institutions" include companies providing financial products and services to consumers, like loans, financial or investment advice, or insurance that collect and receive non-public personal information; e.g.,
 - non-bank mortgage lenders
 - loan brokers
 - some financial or investment advisers
 - tax preparers
 - providers of real estate settlement services
 - debt collectors

THE GLBA

- Who Is Not Subject to the Act
 - The GLBA fails to cover data brokers and third-party processors and servicers.
 - Institutions covered by:
 - federal banking agencies
 - the SEC
 - state insurance authorities
- 

THE GLBA

- Significant Categories of Protection Mandated by the GLBA
 - The Financial Privacy Rule (the "Privacy Rule")
 - Requires financial institutions to disclose and provide written notice of its policies and procedures to its customers, stating how the customer's non-public personal information is protected and shared and providing consumers with a reasonable opportunity to "opt-out" of any information sharing, if required by statute.
 - The Safeguards Rule
 - Requires financial institutions to conduct a thorough risk assessment of its security measures and design a written comprehensive information security program to protect nonpublic personal information in all areas of operation, including administrative, technical, and physical safeguards.

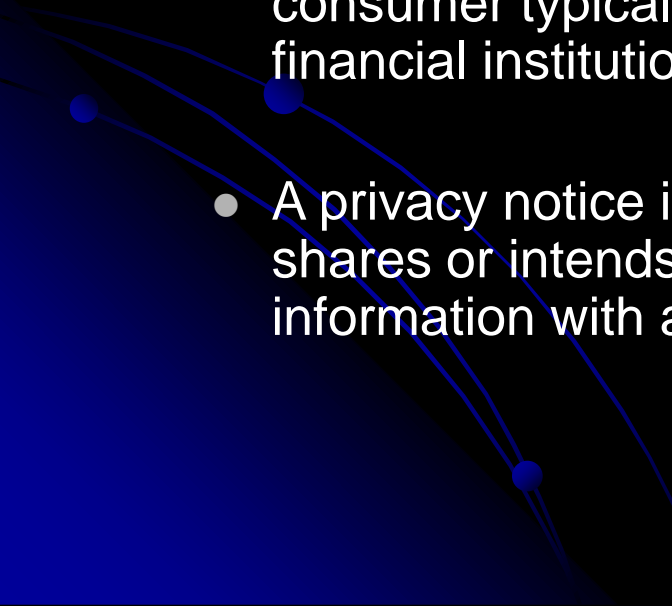
THE GLBA

- Enforcement
 - Civil and criminal actions may be brought by the FTC
 - Civil and criminal penalties for noncompliance include fines and even imprisonment, such as the following:
 - Civil penalties for businesses can include fines up to \$100,000 for each violation
 - Officers and directors can be held personally liable for a civil penalty for up to \$10,000 per violation
 - Criminal penalties may include up to five years in prison

THE GLBA: THE PRIVACY RULE

- Notice Requirements: Content
 - A financial institution must provide notice of its privacy policies and procedures that is "clear and conspicuous."
 - This means the notice must be clear, conspicuous, and accurate, and call attention to the nature and significance of the information within the notice; that is, the notice should:
 - utilize easily readable font,
 - present the information in clear and concise sentences, using definite, everyday words, and
 - include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information.
 - The same rules apply to any changes to a financial institution's privacy policies and procedures.

THE GLBA: THE PRIVACY RULE

- Disclosure Obligations: Type and Frequency of Notice
 - The type and frequency of the notice depends on whether the information belongs to a "consumer" versus "customer."
 - A "consumer" is an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes. A consumer typically has a limited, "one time" connection with the financial institution.
 - A privacy notice is only required when a financial institution shares or intends to share the consumer's nonpublic personal information with a non-affiliated third-party.
- 

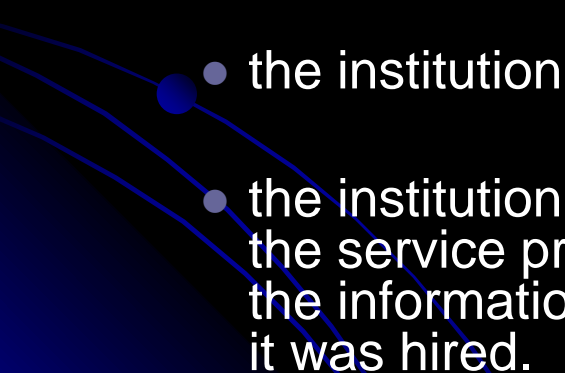
THE GLBA: THE PRIVACY RULE

- Disclosure Obligations: Type and Frequency of Notice
 - A "customer" is a consumer who has a "continuing relationship" with the financial institution.
 - A privacy notice is required as soon as the customer relationship is established, whether or not the financial institution plans to share the consumer's nonpublic personal information with a non-affiliated third-party. In addition, the institution is required to provide its customer with a privacy notice annually for as long as the customer relationship exists.
 - Note: For the purposes of the Privacy Rule, a former customer is considered a consumer.

THE GLBA: THE PRIVACY RULE

- Opt-Out Notice Requirements and Exceptions
 - Requirements
 - A financial institution that intends to share nonpublic personal information with a non-affiliated third-party must provide its consumers notice with an opportunity to opt-out in most instances.
 - The opt-out notice must be delivered to the consumer within a reasonable time and must be included within the privacy notice itself.
 - Like the privacy notice, the opt-out notice must: be clear and conspicuous, state that the consumer has the right to opt-out; and provide a reasonable means by which the consumer may opt-out.

THE GLBA: THE PRIVACY RULE

- Exceptions
 - Service Providers and Joint Marketing
 - The opt-out requirements do not apply when financial institutions share information with service providers who perform certain ordinary business functions such as data processing or servicing accounts as long as:
 - the institution provides an initial notice to the consumer; and
 - the institution enters into a written contractual agreement with the service provider that prohibits it from disclosing or using the information, other than to carry out the function for which it was hired.
- 

THE GLBA: THE PRIVACY RULE

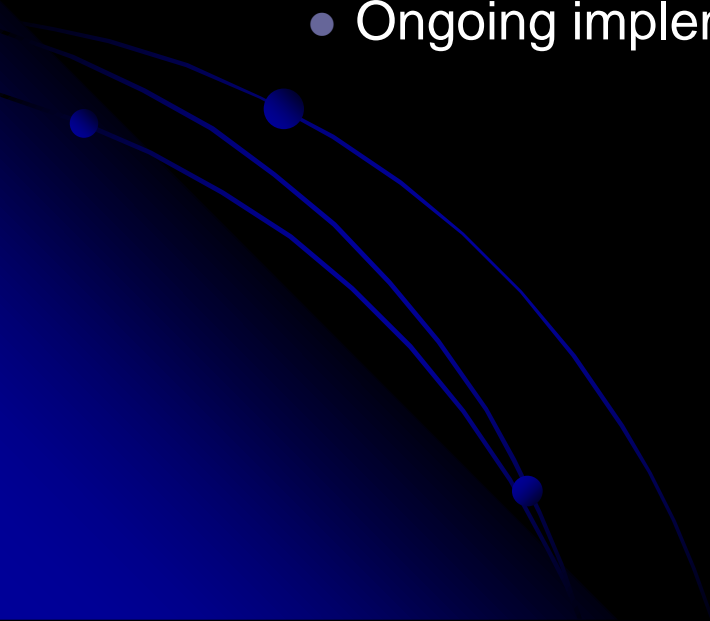
- Exceptions
 - Servicing Transactions
 - The sharing of nonpublic personal information that is necessary for a financial institution to "effect, administer, or enforce" a transaction that a customer requests or authorizes; e.g.,
 - servicing or processing a financial product or service that a consumer requests or authorizes (e.g., loan application);
 - maintaining or servicing the consumer's account, including servicing another entity such as a private label credit card program; or
 - a proposed or actual securitization, secondary market sale (including sale of servicing rights), or similar transaction related to the consumer.

THE GLBA: THE PRIVACY RULE

- Other Exceptions
 - To protect the confidentiality or security of the consumer's records and to protect against or prevent actual or potential fraud.
 - To resolve customer disputes or inquiries.
 - To a consumer's legally appointed representative, such as a pursuant to a power of attorney or persons acting in a fiduciary capacity on behalf of the consumer.
 - To a consumer reporting agency in accordance with the Fair Credit Reporting Act.
 - To comply with all federal, state, or local laws, including court orders.

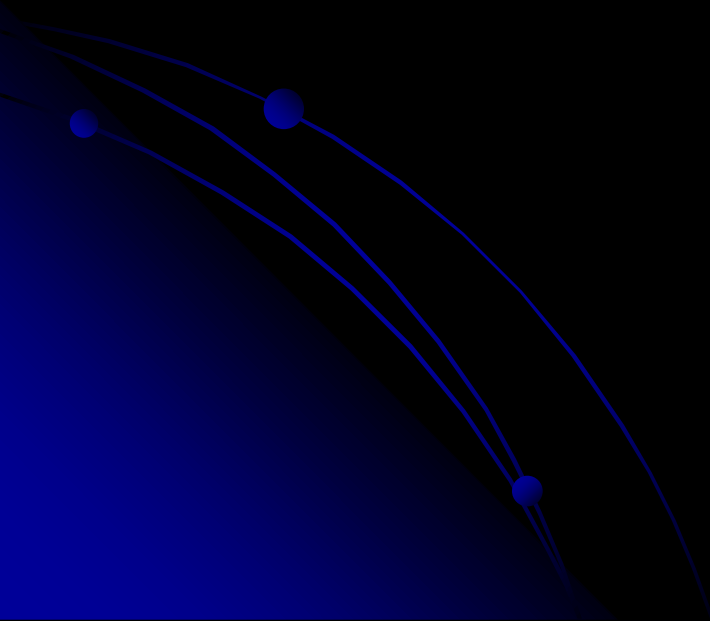
THE GLBA: THE SAFEGUARDS RULE

- Risk Assessment Requirements
 - Develop information security plan;
 - Plan of attack; and
 - Ongoing implementation and maintenance.



THE GLBA : THE SAFEGUARDS RULE

- Additional Considerations in Complying With Risk Assessment Requirements
 - Cost of compliance versus non-compliance
 - Discoverability of risk assessments



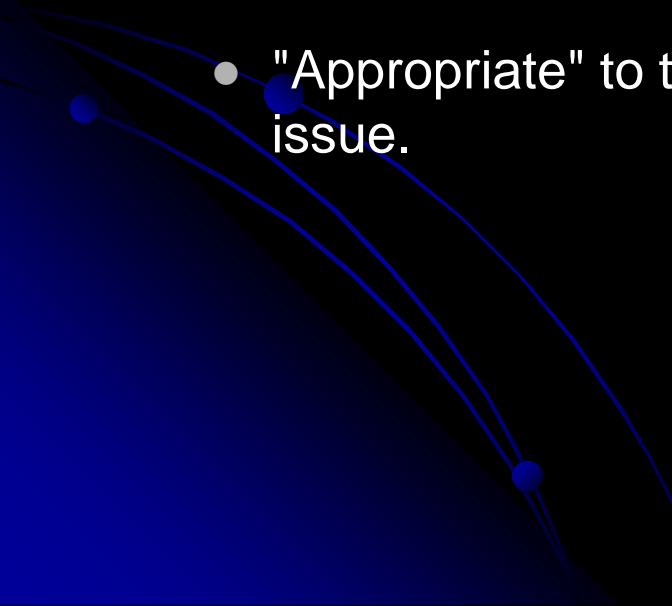
THE GLBA : THE SAFEGUARDS RULE

- Information Security Plan Content
 - Know where sensitive customer information is stored and stored securely.
 - Ensure that the computer or server is accessible only by using a "strong" password and is kept in a physically secure area.
 - Maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area.
 - Take affirmative steps to secure transmission of customer information.
 - Encrypt customer data if it is necessary for you to transmit such information by email or Internet.
 - If you collect information online directly from customers, secure the data transmission automatically.
 - Dispose of customer information consistent with the FTC's Disposal Rule.

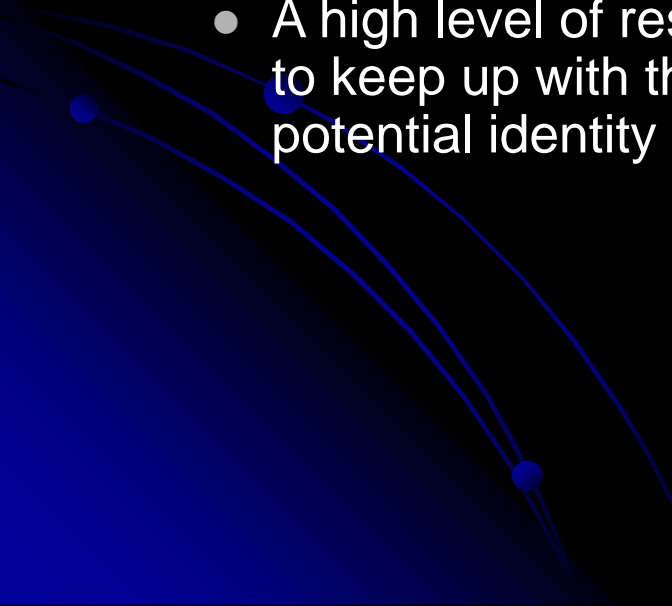
THE GLBA : THE SAFEGUARDS RULE

- Plan for System Attacks Content
 - Monitor the websites of software vendors and relevant industry publications for news about emerging threats and available defenses.
 - Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information.
 - Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.
 - Take affirmative steps to preserve the security, confidentiality, and integrity of customer information and consider notifying consumers, law enforcement, and credit bureaus in the event of a security breach or data breach.
 - Oversee service providers by ensuring that they are able to take appropriate security precautions and in fact do so.
 - Update the security program as necessary in response to frequent monitoring and material changes in the business.

THE GLBA : THE SAFEGUARDS RULE

- Implementation and Maintenance
 - "Appropriate" to the institution's size and complexity;
 - "Appropriate" to the nature and scope of the institution's activities; and
 - "Appropriate" to the sensitivity of the customer information at issue.
- 

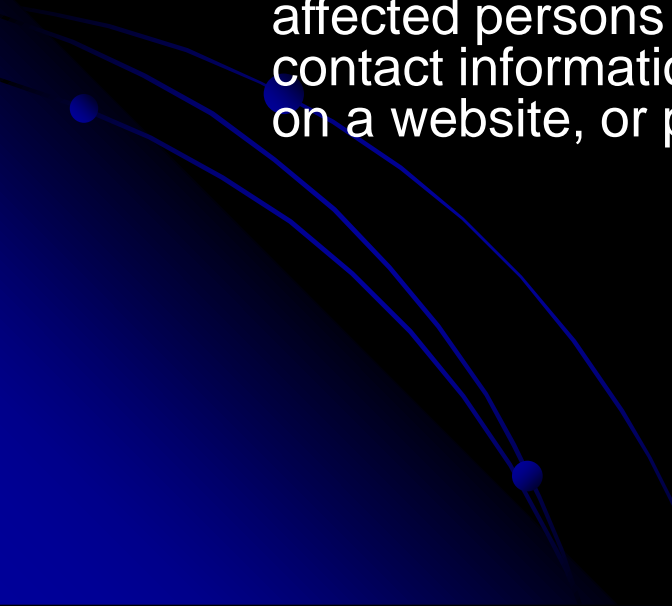
THE GLBA : THE SAFEGUARDS RULE

- Additional Considerations Regarding Security Programs
 - Measure allows for flexibility in developing a security program.
 - Subjective standard may result in selective enforcement, if not unenforceability.
 - A high level of responsibility is placed upon financial institutions to keep up with the latest technology, particularly tools used by potential identity thieves.
- 

THE TEXAS IDENTITY THEFT ENFORCEMENT AND PROTECTION ACT

- Who Is Subject to the Act
 - Every business is required to implement and maintain reasonable procedures to protect "sensitive personal information" collected or maintained in the regular course of business.
 - "Sensitive personal information" is defined as any combination of the following information that is unencrypted:
 - an individual's first name or first initial, and last name +
 - (i) SSN; (ii) DLN or IDN; and/or (iii) account number or credit/debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

THE TEXAS IDENTITY THEFT ENFORCEMENT AND PROTECTION ACT

- What Is Mandated
 - Requires prompt notification of a Texas resident if an unauthorized person has gained access to the resident's sensitive personal information.
 - If the cost of providing notice exceeds \$250,000, the number of affected persons exceeds 500,000, or there is not sufficient contact information, the notice can be given by e-mail, posting on a website, or published notice in statewide media.
- 

THE TEXAS IDENTITY THEFT ENFORCEMENT AND PROTECTION ACT

- Enforcement
 - The Attorney General can bring an action for failure to implement and maintain reasonable procedures to safeguard any sensitive personal information that the business collects or maintains in the regular course of business.
 - The penalties range from \$2,000 to \$50,000 for each violation of this provision.
 - If it appears that a person or business is about to engage in conduct that violates the duty to protect, the Attorney General can also sue to enjoin the violation.
 - The same penalties for failure to protect information also apply to a failure to provide notice of the security breach to affected persons.

THE TEXAS IDENTITY THEFT ENFORCEMENT AND PROTECTION ACT

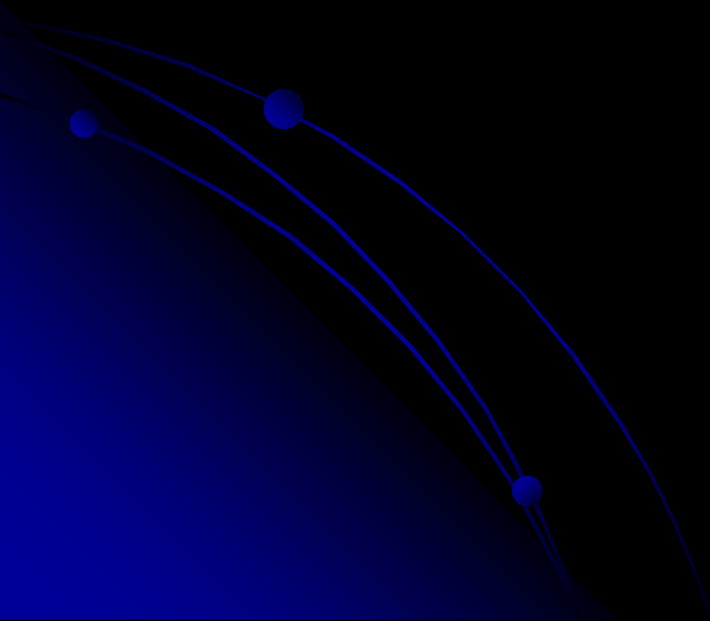
- Related Legislation
 - Section 35.48 of the Business and Commerce Code was amended to prohibit a business from disposing of business records that contain “personal identifying information” until that information is made undecipherable.
 - "Personal identifying information" is defined as:
 - an individual's first name or initial and last name +
 - (A) DOB; (B) SSN or other government-issued IDN; (C) mother's maiden name; (D) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (E) unique electronic identification number, address, or routing code; (F) telecommunication access device, including debit/credit card information; and/or (G) financial institution account number or any other financial information.

POTENTIAL COMMON LAW LIABILITY

- Negligent Enablement of Imposter Fraud
 - This tort theory would impose liability on financial institutions and credit card issuers that fail to follow verification procedures and permit an unauthorized person to obtain credit or some other financial benefit while using another person's information.
 - *Huggins v. Citibank, N.A.* (South Carolina court expressly rejected the imposition of such liability on the basis of a lack of relationship with the issuing entity)
 - *Patrick v. Union State Bank* and *McCowan v. Warner* (Alabama court imposed a duty on financial institutions when a special relationship exists between the victim and the alleged tortfeasor; such as where the alleged identity theft victim is actually a customer of the institution that did not adequately safeguard sensitive information from theft by a dishonest employee)

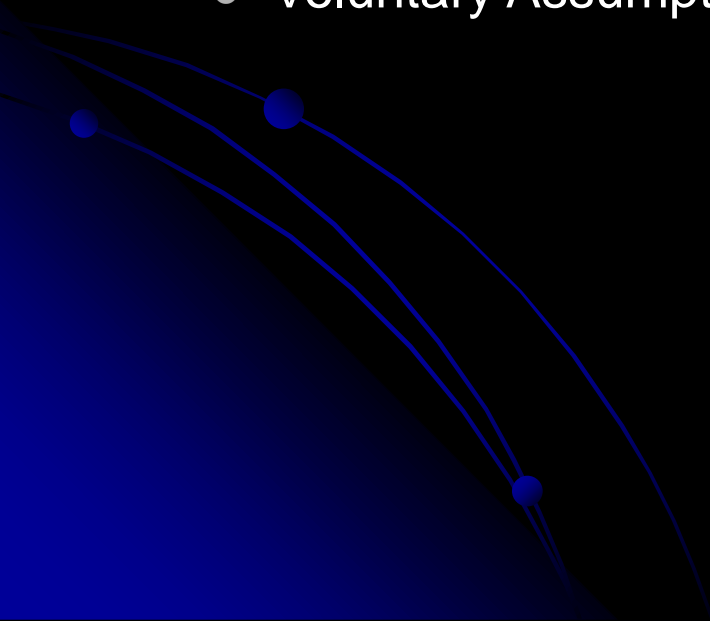
POTENTIAL COMMON LAW LIABILITY

- Implied Contract
 - In *Richardson v. DSW, Inc.* (Illinois federal district court recently allowed an implied contract cause of action to survive a 12(b)(6) Motion to Dismiss in connection with a data theft incident of credit card and purchase information had been stolen from a shoe store's computer system)

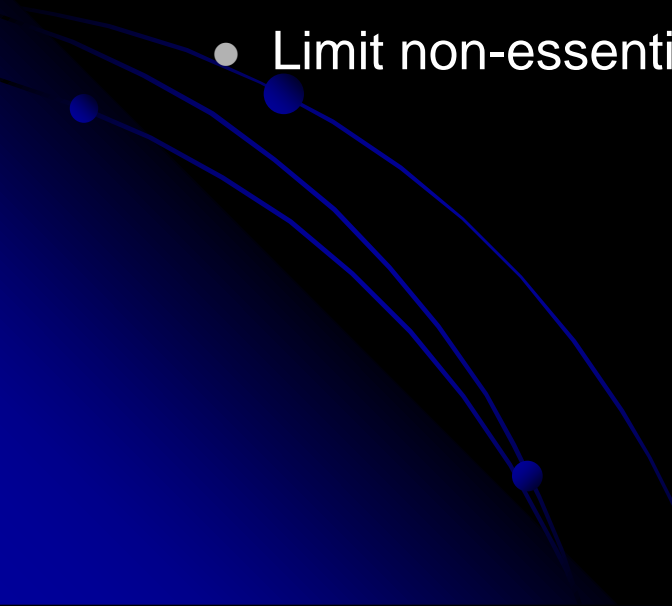


POTENTIAL COMMON LAW LIABILITY

- Other Potential Theories on the Horizon
 - Common Duty to Protect
 - Negligence Per Se
 - Voluntary Assumption of the Duty



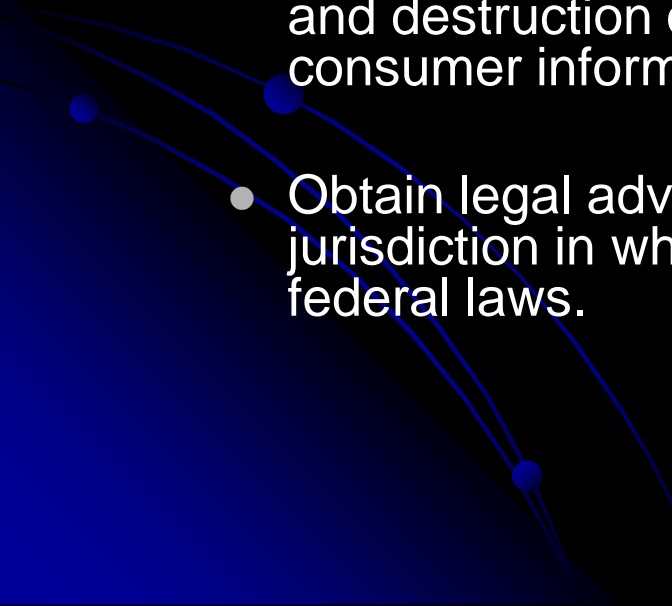
WHAT YOU CAN DO TO PROTECT YOUR BUSINESS

- Preventing Data Breaches
 - Evaluate the need to collect and keep customer information. If the information, such as social security numbers and birthdates, are unnecessary to a business function, or if other unique identifiers can be created to avoid collecting such data, then sensitive information probably should not be collected.
 - Limit non-essential employee access to sensitive information.
- 


WHAT YOU CAN DO TO PROTECT YOUR BUSINESS

- Conduct employee training and management that include:
 - check employee references and perform background checks;
 - require employees to sign a confidentiality agreement;
 - limit employee access to sensitive customer information;
 - use password-activated screen savers to lock employee computers;
 - encrypt customer files on laptops and other computers in case of theft;
 - impose disciplinary measures for security policy violations;
 - prevent terminated employees from accessing customer information by immediately deactivating their passwords or user names.

WHAT YOU CAN DO TO PROTECT YOUR BUSINESS

- Store sensitive information in physically or technologically secure locations. This means encrypting electronic data, locking physical documents up, limiting access, and outsourcing computer security functions to a company with appropriate experience.
 - Dispose of nonpublic personal information by burning, pulverizing, or shredding of consumer information in paper form and destruction or erasure of electronic media containing consumer information.
 - Obtain legal advice as to the applicable privacy laws in each jurisdiction in which you conduct business as well as applicable federal laws.
- 

WHAT YOU CAN DO TO PROTECT YOUR BUSINESS

- Other Risk Management Considerations
 - Security and Privacy Insurance
 - Coverage Available
 - Failure of network security
 - Failure to protect or wrong disclosure of private information
 - Failure to protect personally identifiable information from misappropriation
 - Violation of federal, state, or local privacy laws alleged in connection with a failure to protect private information
- 

WHAT YOU CAN DO TO PROTECT YOUR BUSINESS

- Indemnity Agreement
 - Important Considerations
 - Express Negligence Rule
 - Is it worth the paper its written on?
- 