Compliance with the Gramm-Leach-Bliley (Financial Services Modernization Act of 1999)

The **Gramm-Leach-Bliley Act** (GLB) was passed in 1999 to protect the privacy and security of nonpublic, personal information collected by financial institutions about consumers. Education originally thought they were excluded and petitioned for exclusion due to coverage of FERPA and HIPPA. Partial relief was granted.

There are two sections:
Section 313, which defines financial institutions and describes **privacy** requirements
Section 314, which requires security to **safeguard** nonpublic, non-directory information.

Universities are exempt from Section 313 if they are in full compliance with FERPA and HIPPA. Universities are not exempt from Section 314 regulation as financial institutions.

The Federal Trade Commission (FTC) administers the Act and the regulations are effective May 23, 2003.

The law allows flexibility within institutions as to how it is implemented, but grants no "safe harbors" since institutions should develop policies based on their practices.

Enforcement will be by the FTC. Initial enforcement will be large-scale violations. Industries will be selected where risks are great and breach anticipated. Media coverage of a breach could trigger enforcement audit.

What Type of Information is covered by this act?

Names
Address
Phone Numbers
Credit Card Account Number
Income and credit history (Financial Aid or Loan Application)
Payment History/Account Balances
Social Security Number
Passwords/PIN that provide security to any of the above.

What must TCU do to be in compliance?

1.) Identify one or more individuals to coordinate an information security program.
2.) Identify foreseeable internal and external risks to security
3.) Develop a written plan for information safeguarding
4.) Perform a risk analysis/assessment to determine compliance
5.) Take steps to modify procedures
6.) Train employees with access to information
7.) Inform "customers" of opt-out option, if applicable
8.) Require "service providers" to implement and maintain safeguards
9.) Review policy/procedures and make appropriate modifications

What are some examples of inadvertent exposure of breach?

1.) Using as scratch paper something that has confidential information on the back.
2.) Using Social Security Number where not necessary (required for Tax purpose)
3.) Writing someone's credit card number down where others could steal

4.) Recycling confidential information without shredding