Overview of Financial Privacy Laws

Federal:
- Right to Financial Privacy Act of 1978
- Gramm-Leach-Bliley Act of 1999
- Fair and Accurate Credit Transactions Act of 2003

Wisconsin:
- Case Law
- Wis. Stat. 214.37
Right to Financial Privacy Act of 1978

- Protects the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records.

- Reaction to the U.S. Supreme Court’s 1976 ruling in *United States v. Miller*, where the Court found that bank customers had no legal right to privacy in financial information held by financial institutions.

RFPA Cont’d.

No Governmental Access Unless:

- Customer has authorized disclosure;
- There is an appropriate subpoena or summons;
- There is a qualified search warrant; or
- There is an appropriate written request from an authorized government authority.
RFPA Cont’d.

Exceptions (examples):
• Disclosures do not identify a particular customer.
• Disclosures in the financial institutions interest (i.e. perfecting security interests, obtaining loan guaranties, etc.).
• Disclosures in connection with supervisory investigations,
• Emergency disclosures and disclosure to federal agencies charged with national security functions.

Civil Penalties:
• $100/violation.
• Actual damages sustained.
• Punitive damages as the court may allow.
• Costs and attorney’s fees.
• Disciplinary action.

Injunctive Relief:
• Injunctive relief available.
• Costs and attorney’s fees.
Gramm-Leach-Bliley Act

Gramm-Leach-Bliley Act ("GLBA"), Intent:
• GLBA seeks to protect consumer financial privacy.

Three Primary Privacy Components:

• Financial Privacy Rule - Governs the collection and disclosure of customers’ personal financial information by financial institutions.
• Safeguards Rule - Requires all financial institutions to design, implement and maintain safeguards to protect customer information
• Pretexting provisions - Protects consumers against having their personal financial information obtained under false pretenses.

GLBA Cont’d.

Who must comply?

• First, Financial institutions that collect nonpublic personal information from customers or consumers.

• Second, recipients of nonpublic personal information from a financial institution with which they are not affiliated.
GLBA Cont’d.

• Financial institution:
  – Any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956.

• Nonpublic personal information:
  – Personally identifiable financial information.

• Consumer:
  – An individual who obtains a financial product or service that is to be used primarily for personal, family, or household purposes, or that individual’s legal representative.

• Customer:
  – A consumer who has a customer relationship (continuing relationship) with you.

GLBA Cont’d. – Privacy Rule

• Requires a financial institution in specified circumstances to provide notice to customers and consumers about its privacy policies and practices.

• Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties.

• Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by “opting out” of that disclosure, subject to certain exceptions.
GLBA Cont’d. – Privacy Rule

**Initial notice:**
- Must provide a clear and conspicuous notice that accurately reflects privacy policy to:
  - Customers; and
  - Consumers only if the company shares the information with nonaffiliated third parties.

**Annual notice:**
- Must be given to customers.
- Annual means at least once in any period of 12 consecutive months during which the relationship exists.

**Procedural Considerations:**
- Privacy Notice must be delivered in writing, or electronically if agreed.
- Opt-Out Notice must describe “reasonable means” to opt-out (i.e. toll-free telephone no., detachable form, etc.).
GLBA Cont’d. – Privacy Rule

Exceptions:
– For use by service providers and in joint marketing efforts.
– For processing and serving transactions.
– To protect against fraud or unauthorized transactions, or as provided in response to a court order.
– Where the institution reasonably believes the information is publically available.

GLBA Cont’d. – Privacy Rule

Miscellaneous:
• Does not modify, limit, or supersede the operation of State law except to the extent inconsistent, and State law can offer greater protections.

• FTC may bring enforcement actions for violations of the Privacy Rule in federal district court.
GLBA Cont’d. – Safeguard Rule

- The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information.

- The plan must be appropriate to the company’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

Compliance:

- Designate employee(s) to coordinate a security program.
- Identify the risks to customer information, and evaluate the effectiveness of the current safeguards for controlling those risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm’s business or operations, or the results of security testing and monitoring.
GLBA Cont’d. – Pretexting

• Aimed at stopping third parties from obtaining personal information through false pretenses.

• Under the GLBA, a person or company can’t use false or fraudulent statements, or forged, lost, or stolen documents, to get your personal information from a financial institution or from you personally.

Fair and Accurate Credit Transactions Act of 2003

• Amends certain provisions of the Fair Credit Reporting Act.

• Designed to provide consumers with the ability to safeguard their sensitive, personally identifiable financial information and to grant Federal Trade Commission with enforcement tools.
FACTA Cont’d.

Red Flags Rule:
• Requires financial institutions and some creditors to conduct a periodic risk assessment to determine if they have covered accounts.
• Implement a program to detect red flags if they have covered accounts.

Disposal Rule:
• Requires that information be burned, pulverized, or shredded and may include the destruction or permanent erasure of electronic records.

FACTA Cont’d.

Financial Institution:
• A State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer.

Covered Account:
• An account that a financial institution or creditor offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions...

• Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identify theft...
FACTA Cont’d. – Red Flags Rule

Compliance:
• Each financial institution or creditor that offers or maintains covered accounts must develop and implement a written Identity Theft Prevention Program ("Program") that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.
• Program should be appropriate for size and complexity of institution and nature and scope of activities.

FACTA Cont’d. – Red Flags Rule

Program Elements:
• Identifies relevant Red Flags and incorporates them into Program.
• Detect Red Flags that have been incorporated into Program.
• Respond appropriately to any Red Flags.
• Ensure Program is updated periodically to reflect changes in risks to customers.
FACTA Cont’d. – Red Flags Rule

Implementation:
• Obtain approval of the initial written Program from board of directors or committee.
• Involve BOD, committee, or a designated senior manager in the oversight, development, and implementation of Program.
• Train staff as necessary.
• Exercise appropriate and effective oversight of service provider arrangements.

FACTA Cont’d. – Red Flags Rule

Benefits of Compliance:
• Lower risk of lawsuit.
• Lower risk of operational fraud.
• Lower risk of identify theft.
• Increased customer satisfaction/approval.
FACTA Cont’d – Red Flags Rule

Noncompliance Penalties:
• Federal Enforcement by the FTC.

• State Enforcement by the State Attorney General’s Office.

• Civil lawsuits by consumers.

FACTA Cont’d. – Disposal Rule

• Designed to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information.

• Applies to any person over which the FTC has jurisdiction, that, for a business purpose, maintains or otherwise possesses consumer information.
FACTA Cont’d. – Disposal Rule

Disposal Rule, Compliance:
• Must take reasonable measures to protect against unauthorized access to or use of information in connection with its disposal.
  – Implementing and monitoring compliance with policies burning, pulverizing, or shredding of papers or erasing electronic media.
  – Monitoring third parties retained to destroy documents.

Wisconsin Case Law

• State v. Starke, 81 Wis. 2d 399 (1977).

• State v. Gilbertson, 95 Wis. 2d 102 (1980).

• First Nat’l Bank & Trust Co. v. Notte, 97 Wis. 2d 207 (1980)
Wis. Stat. s. 214.37

• A savings bank, which is regulated by the state, must keep its financial records confidential.

• A person has the right to inspect any records maintained by the bank concerning that person’s deposit accounts or loans, and may authorize others to have access to these records.

Wis. Stat. 214.37 Cont’d.

Absent Authorization, Disclosure Limited to Following:

• To an officer, employee or agent of the savings bank to prepare, examine, handle, or maintain, or a certified public accountant engaged by the savings bank to perform an audit.

• To an officer, agent or employee of the state division of banking or other government authorized banking organization.

• As part of the regular exchange of credit information the savings bank and other financial institutions, a mortgage broker, or a consumer reporting agency.

• As information furnished to the appropriate law enforcement authority if the savings bank believes a crime has been committed involving the savings bank.

• Furnished pursuant to legal process, such as subpoena, summons warrant or court order.

• Where disclosure is required by state or federal law.
Wis. Stat. 214.37 Cont’d.

Requirements for Sale or Use:

• Does not classify customer by individual financial criteria and contains only the names and addresses of customers.

• Each customer gets prior written notice of savings bank’s intent to furnish information about the customer, and is informed of the right to prevent the release by notifying savings bank.

• The person who is furnished a list agrees in writing not to furnish the list to another person.

Resources:


Questions?

Attorney D. Clarke Sugar
Axley Brynelson, LLP

csugar@axley.com
608.260.2481
www.axley.com