

**Customer Privacy  
How to Avoid the Disaster in the Making  
MBA's Document Custody Conference  
September 19, 2006  
Seattle, WA**

**Meg Zaleski**  
**JP Morgan Chase Bank, NA**  
**Vice President and Assistant General Counsel**  
**[Meg-zaleski@chase.com](mailto:Meg-zaleski@chase.com)**

- **Privacy Breach as potential “disaster”.**
- **How did we get where we are today?**
- **The current legal and regulatory climate.**
- **What the future holds.**

- **The “right” of privacy**
- **Political Freedom**
- **Freedom from Intrusion**
- **Personal Autonomy – The right to be left alone**
- **Access to and Use of Personal Information**
- **Marketing Initiatives and the Information Super Highway**
- **Privacy vs. Security**

- **What is personal information?**
- **Who owns it?**
- **Who can it be shared with?**
- **How can it be used?**

# Statutory and Regulatory Scheme



- Gramm-Leach-Bliley Act (GLB) (2000)
- Fair Credit Reporting Act (FCRA) (1971)
- Fair and Accurate Credit Transactions Act (FACT Act) (2003)
- California Financial Information Privacy Act (SB-1) (2004)
- Telemarketing Acts and Regulations
  - » FTC: Telemarketing and Consumer Fraud and Abuse Act; Telemarketing Sales Rule
  - » FCC: Telephone Consumer Protection Act
  - » Various state laws.
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
- Others

# Gramm-Leach-Bliley Act and Regulation P



- Declares that it is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of customers' non-public personal information.
- Applies to financial institutions – banks, mortgage lenders, insurance companies, financial and investment advisors.
- Protects individuals who obtain financial products and services for personal, family or household purposes.
- “Consumer” – Individual (or legal representative) who obtains financial products or services from a financial institution for personal, family or household purposes (e.g. an applicant, even if credit is not extended).
- “Customer” – A Consumer who has entered into and maintains an ongoing relationship with a financial institution (e.g. deposit account, mortgage loan).

# Gramm-Leach-Bliley Act and Regulation P



- Protects information that is “personally identifiable financial information” that is not publicly available.
- Information furnished by or about the consumer in connection with the transaction – even if the information is not strictly financial.
- Fact that an individual is your customer (unless publicly available)
- Information collected from internet cookies.
- “Publicly Available Information” is excluded. Financial institutions must have reasonable basis to believe that the information is lawfully available to the public.

## **PROVIDE PRIVACY NOTICE**

- **Initial**
  - To Customers – Not later than when the customer relationship is established.**
  - To Consumers – Before disclosing non-public personal information to unaffiliated third party.**
- **Annual**
  - To Customers – Within 12 month periods on a consistent basis for as long as the relationship exists.**
- **Revised Notices**
  - If you change your policy.**

## **PROVIDE PRIVACY NOTICE**

- **“Clear and Conspicuous”**
- **Must be reasonably understandable and designed to call attention to the nature and significance of the information.**
- **Provide in writing, electronically if consumer agrees, and in a manner that the individual can reasonably be expected to receive actual notice.**

# Obligations of Financial Institutions



## **PRIVACY NOTICE MUST INCLUDE**

- **Categories of non-public personal information collected.**
- **Categories of non-public personal information that may be disclosed.**
- **Categories of parties – affiliated and non-affiliated – to whom non-public personal information may be disclosed.**
- **Policy on disclosing information about former customers**
- **Whether information will be disclosed to service providers and joint marketers.**
- **Right to Opt Out.**
- **FCRA affiliate sharing disclosures.**
- **Policies with respect to protecting the confidentiality and security of non-public personal information.**

## OPT OUT NOTICE

- **Inform consumer that the financial institution may disclose non-public personal information to non-affiliated third parties and consumer has a right to prevent disclosure.**
- **Provide reasonable means of exercising opt out right.**
- **Provide reasonable time for customer to opt out before disclosing information.**
- **Opt out is effective until revoked.**

## OPT OUT NOTICE EXCEPTIONS

- **Routine Business**
  - » **Effect, administer or enforce a transaction.**
  - » **Maintain or service an account.**
  - » **Secondary marketing or M&A.**
  - » **Prevent fraud or comply with law.**
  
- **Service Providers**
  
- **Joint Marketers**

# Fair Credit Reporting Act



## PURPOSE

- **Provide rules for access to and use of personal information.**
- **Promote fair and accurate collection and reporting of information.**
- **Ability to view and dispute.**
- **Limits on use and dissemination.**
- **Balance privacy impact vs. benefit to consumer.**

## **DEFINITIONS**

- **Consumer Report – Communication of information by a consumer reporting agency that bears on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer’s eligibility for**
  - **Credit or insurance for personal, family or household purposes;**
  - **Employment;**
  - **Certain other authorized purposes.**

## “Consumer Report” does not include:

- **A report containing information solely about transactions or experiences between the consumer and the institution making the report.**
- **Communication of transaction and experience information among affiliates.**
- **Communication of other (non-T&E) information among affiliates if consumer has been given notice and opportunity to opt out.**
- **Communication of credit decision to interested third party.**
- **Miscellaneous others.**

## “Consumer Reporting Agency”

- **Person who, for monetary fees, dues, or on a cooperative basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.**

## **PERMISSIBLE PURPOSES OF OBTAINING CREDIT REPORTS**

- **In accordance with the written instructions of the consumer.**
- **For use in connection with a credit transaction requested by the consumer; as a potential investor or servicer of an account; review of existing accounts; legitimate business need in connection with transaction requested by the consumer.**
- **Pre-approved offerings if certain conditions are met.**

## CONSUMER PROTECTIONS

- **Adverse action notices.**
- **Right to dispute and correct information.**
- **Right to notice and opportunity to opt out of information sharing among affiliates.**

# Fair Credit Reporting Act Information Sharing Delivery of Privacy Notice



	Type of Information		
Uses of Information for:	Transaction & Experience Information	Non-Transaction & Non-Experience Information <sup>[1]</sup>	Credit Report
<ul style="list-style-type: none"> <li>•Statistical analysis &amp; modeling</li> <li>•FCRA: Customer Opt Out</li> </ul>	FCRA: OK to share	FCRA: OK to share	FCRA: OK to share
<ul style="list-style-type: none"> <li>•Product Eligibility</li> <li>•FCRA: Customer Opt Out</li> </ul>	FCRA: OK to share	FCRA: Can't share	FCRA: Can't share
<ul style="list-style-type: none"> <li>•Marketing</li> <li>•FCRA: Customer Opt Out</li> </ul>	FCRA: OK to share	FCRA: OK to share	FCRA: Can't share

## Fair and Accurate Credit Transaction Act of 2003 (FACT Act)



- **Blurring of distinctions among privacy, credit data, identity theft and security concerns – possible launch point for public policy issues regarding access, ownership and control of consumer data.**
- **Made permanent certain provisions of FCRA that were scheduled to sunset on January 1, 2004.**
- **Applied federal pre-emption to information sharing and credit reporting.**

# Fair and Accurate Credit Transaction Act of 2003 (FACT Act)



## **NEW IDENTITY THEFT PROTECTIONS**

- **Must have reasonable procedures in place to respond to notice from credit reporting agency that account information may be the result of identity theft.**
- **If you have provided credit to a person who allegedly committed identity theft you must notify the victim and cooperate in any investigations.**
- **Must implement procedures to investigate and reconcile if a notice of address discrepancy is received from credit bureau.**
- **Consumers can request that initial fraud alert, extended fraud alert, or active duty alert be placed in their credit file. Lender must take reasonable steps to confirm identity of applicant before extending credit.**
- **Information in credit report which consumer identifies as resulting from identity theft must be blocked.**

# Fair and Accurate Credit Transaction Act of 2003 (FACT Act)



## DISCLOSURES

- **Credit Score Disclosure required if credit score is considered in making residential mortgage loan.**
- **If risk based pricing is used, must disclose impact of credit report / score.**
- **Consumer entitled to one free credit report per year.**

# Fair and Accurate Credit Transaction Act of 2003 (FACT Act)



## ASSURANCES OF ACCURACY

- **If you submit negative credit information about a consumer to a credit bureau, you must disclose this to the consumer.**
- **Must implement procedures ensuring the accuracy of information reported to credit bureaus – Do not submit if there is “reasonable cause to believe” the information is not accurate.**
- **Implement procedures to address treatment of information reported to be inaccurate.**

# Fair and Accurate Credit Transaction Act of 2003 (FACT Act)



## MARKETING

- **If you use a credit report to make an unsolicited offer of credit to a consumer you must provide certain notices and the opportunity to opt out of future solicitations from you and others.**
- **Affiliate sharing provisions of FCRA remain in effect, but notice and opt out is required before shared information can be used for marketing.**
- **Opt out effective for five (5) years.**
- **Exceptions for pre-existing business relationship, information used to perform services on behalf of an affiliate, solicitation authorized or requested by the consumer.**

# Fair and Accurate Credit Transaction Act of 2003 (FACT Act)



Type of Information			
Uses of information for:	Transaction & Experience Information	Non-transaction & Non-Experience Information <sup>1</sup>	Credit Report
<ul style="list-style-type: none"> <li>•Statistical analysis &amp; modeling</li> <li>•FCRA: Customer Opt's Out</li> <li>•FACT: Customer Opt's Out</li> </ul>	<p>FCRA: OK to share FACT: Not applicable</p>	<p>FCRA: OK to share FACT: Not applicable</p>	<p>FCRA: OK to share FACT: Not applicable</p>
<ul style="list-style-type: none"> <li>•Product Eligibility</li> <li>•FCRA: Customer Opt's Out</li> <li>•FACT: Customer Opt's Out</li> </ul>	<p>FCRA: OK to share FACT: Not applicable</p>	<p>FCRA: Can't share FACT: Not applicable</p>	<p>FCRA: Can't share FACT: Not applicable</p>
<ul style="list-style-type: none"> <li>•Marketing</li> <li>•FCRA: Customer Opt's Out</li> <li>•FACT: Customer Opt's Out</li> </ul>	<p>FCRA: OK to share FACT Act: OK to share but can't use for marketing<sup>2</sup></p>	<p>FCRA: OK to share FACT Act: OK to share but can't use for marketing<sup>2</sup></p>	<p>FCRA: Can't share FACT Act: OK to share but can't use for marketing<sup>2</sup></p>

## COMMENTARY:

- The most significant additional limitations imposed by the FACT Act opt out are depicted in the boxes for “Use for Marketing” of (a) Transaction/Experience Information and (b) Non-Transaction/Experience Information. Legal counsel should first review specific information sharing programs.
  1. This category includes application information and purchased information..
  2. Exceptions to the FACT Act limitation include those circumstances where the company using the affiliate’s information for marketing: (a) has a pre-existing business relationship with the consumer, (b) is responding to a communication initiated by the consumer, (c) is acting as a service provider for the affiliate.

## California Information Privacy Act (SB-1 – 2004)



- **Applies to financial institutions providing financial products and services to California residents for personal, family or household purposes.**
- **OPT IN is required for sharing customer information with non-financial third parties.**
- **OPT OUT is required for sharing with financial third parties.**
- **OPT OUT is required for sharing information with affiliates unless the affiliate has the same regulator, is in the same line of business, and has a shared brand name.**
- **Court challenge in process regarding FACT Act pre-emption.**

**FTC Telemarketing and Consumer Fraud and Abuse Act; Telemarketing Sales Rule. Covers telemarketing vendors.**

**FTC Telephone Consumer Protection Act (TCPA). Covers financial institutions. Regulates faxes and cell phones as well as telephone calls.**

## **VARIOUS STATE LAWS**

- **TCPA pre-empts portions of state laws with respect to interstate calls.**
- **More restrictive provisions of state law apply to intrastate calls.**
- **“Telemarketing” defined – The initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods or services.**
- **Rule – No telemarketing sales calls may be made to consumers whose names appear on the National Do Not Call list. Penalty for violations is \$11,000 per call.**

## EXCEPTIONS

- **Calls to existing customers with whom there is an “established business relationship” through voluntary two-way contact based on this consumer’s purchase or transaction with the caller within the last 18 months.**
- **Established business relationship based on the consumer’s inquiry or application within the last 3 months. Nature of inquiry must be such that consumer would expect a call.**
- **True service calls.**

## RELATED REQUIREMENTS

- **Scripting – Caller must give his/her name, entity on whose behalf the call is made, and number to call to record caller-specific DNC requests.**
- **Restricted calling hours.**
- **Caller ID – Blocking is prohibited. Outbound calls must show caller's business telephone number and the name of the company on whose behalf the call is being made.**

- **“Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003” effective January 1, 2004.**
- **Transmission of commercial e-mail messages is permitted as long as the sender complies with a list of Do’s and Don’t’s .**
- **Pre-empts state laws.**

## **Transaction/Service E-Mails – Email messages the primary purpose of which is:**

- » **To facilitate, complete or confirm a commercial transaction.**
- » **To provide warranty, product recall or safety and security information with respect to a commercial product or service used or purchased by the recipient.**
- » **To provide notification concerning a change in terms or features, standing or status, or account balance or statement information regarding a subscription, membership, account, loan or other ongoing commercial relationship.**
- » **To provide information directly related to an employment relationship or related benefit plan involving the recipient.**
- » **To deliver goods or services including updates and upgrades that recipient is entitled to receive under a previous transaction.**

**Marketing/Commercial Emails – A commercial e-mail message the primary purpose of which is to advertise or promote a commercial product or service, including content on an internet website operated for a commercial purpose.**

## CAN SPAM – E-Mail Do's and Don'ts



- **DON'T use false or misleading headers.**
- **DO identify the computer the email came from.**
- **DON'T use a misleading subject headline.**
- **DO clearly display a return email message or other online opt out mechanism that is operative for 30 days.**
- **DO honor opt out requests in 10 business days unless the consumer gives subsequent consent to receive further emails.**
- **DO clearly display an indication that it is a commercial solicitation or advertisement – unless the consumer has given affirmative consent to receive it.**
- **DO include the postal address of the sender.**
- **DON'T use high tech intrusions – dictionary attacks, harvesting addresses, etc.**

- **FTC and other federal regulators (OCC, SEC, etc.)**
- **State AGs – Deceptive Trade Practice**
- **No Individual Actions – No Class Actions**
- **Statutory Damages**
- **Commercial emails x \$250 not to exceed \$2 million**
- **> If aggravated circumstances (treble damages)**
- **< If compliance procedures are in place**
- **Injunctive Relief**
- **Criminal penalties for fraud or predatory practices**

**States are increasingly active in passing laws on privacy-related issues.**

- **Telemarketing**
- **Security Breaches**
- **Email**
- **Limits on sharing financial information**
- **Restrictions on use of social security numbers**
- **Security freezes**

- **Federal data breach legislation**
- **Microsoft proposal – GLB-like privacy legislation for non-financial institutions**
- **Credit mining**
- **New form of privacy policy**