

PRIVACY SUBCOMMITTEE

**American Bar Association
Committee on Consumer Financial Services
Privacy Subcommittee
Winter Meeting – Scottsdale, Arizona
January 11, 2008**

PRIVACY SUBCOMMITTEE

Chair: Patricia E.M. Covington, Hudson Cook, LLP, Hanover, MD

Vice Chair: Obrea Poindexter, Morrison & Foerster LLP, Washington, DC

Presentation: *Implementation of Affiliate Sharing Rule and Red Flag Rule*

Speakers:

Anne Fortney, Hudson Cook, LLP, Washington, DC
Peter Gilbert, Capital One Services, McLean, Virginia
David Stein, Federal Reserve Board, Washington, DC

Affiliate Marketing Rule
Anne P. Fortney
Hudson Cook, LLP

I. Overview

The Fair and Accurate Credit Transactions Act (“FACT Act”) amended the Fair Credit Reporting Act (“FCRA”) to regulate the use of certain consumer information by affiliates for marketing solicitation purposes (“affiliate marketing”), and it required the federal banking agencies, the National Credit Union Administration, and the Federal Trade Commission (“Federal Agencies”) to issue a joint rule governing affiliate marketing. The Federal Agencies published their final rule on October 30, 2007, with compliance mandatory beginning October 1, 2008.¹

The rule creates certain notice and opt out rights for consumers when their “eligibility information” is (a) obtained by a company, (b) shared with one or more affiliates of the company and (c) to be used by the affiliate to make a solicitation for marketing purposes to the consumer. If the affiliate lacks a “pre-existing business relationship” with the consumer, the affiliate may not use the eligibility information make the solicitation unless (a) the consumer has been given both notice of the right to opt out of having her information used to make such solicitations and a reasonable opportunity to opt out, and (b) the consumer has not opted out.

II. Background for Discussion of Compliance Issues

A. Scope. Applies to any person subject to the respective jurisdiction of one of the Federal Agencies. The FTC’s rule applies to any person over which the FTC has jurisdiction that uses information from its affiliates for the purpose of marketing solicitations, or provides information to its affiliates for that purpose.

B. Key Definitions

1. “Affiliates” are companies related by common ownership or common corporate control.
2. “Eligibility information” means any information the communication of which would be a consumer report if the FCRA section 603(d)(2)(A) exclusions from the definition of “consumer report” did not apply.
 - a. *Examples:*
 - i. Credit report information shared with affiliates pursuant to the FCRA notice and opt-out under FCRA.

¹ 72 FR 61424 (Oct. 30, 2007).

- ii. An affiliate's transactions or experiences with a consumer when the communication of that information to a third party would be a consumer report.
 - b. *Exclusions*. The definition expressly excludes aggregate or blind data that does not contain personal identifiers such as account numbers, names, or addresses.
3. "Pre-existing business relationship" is a relationship with a consumer based on:
- a. a financial contract between the person and the consumer which is in force on the date the consumer is sent a solicitation;
 - b. the purchase, rental, or lease by the consumer of the person's goods or services, or a financial transaction with the consumer during the 18-month period immediately preceding the date the consumer is sent a solicitation; or
 - c. an inquiry or application by the consumer regarding a product or service during the three-month period immediately preceding the date the consumer is sent a solicitation.
4. A "solicitation" means the marketing of a product or service initiated by an affiliate to a consumer that is based on eligibility information from its affiliate and intended to encourage the consumer to purchase or obtain the product or service.
- a. The definition applies to marketing material that is targeted to particular consumers based on eligibility information, such as a telemarketing call, direct mail and email.
 - b. It excludes generalized marketing material that is not so targeted, such as television, general circulation magazines and billboard advertisements.

C. Affiliate Marketing Opt-Out

1. *General Rule*. A person subject to the rule may not use eligibility information about a consumer received from an affiliate to make a solicitation for marketing purposes to the consumer, unless—
- a. It is clearly and conspicuously disclosed to the consumer in writing or, if the consumer agrees, electronically, in a concise notice that the person may use eligibility information about that consumer received from an affiliate to make solicitations for marketing purposes to the consumer;

- b. The consumer is provided a reasonable opportunity and a reasonable and simple method to opt out of the use of eligibility information to make solicitations for marketing purposes; and
 - c. The consumer has not opted out.
2. “*Making solicitations*” occurs when –
- a. a person receives eligibility information from an affiliate;
 - b. the person uses that eligibility information to identify recipients of a solicitation, or establish criteria used to select recipients of a solicitation or decide which of its products or services to market to the consumer; and
 - c. the consumer is provided a solicitation as a result of the company’s use of the eligibility information.
3. *Receipt of eligibility information.* As described in the “making solicitations” section immediately above:
- a. A person may receive information from an affiliate directly or through a common database.
 - b. A person may also receive eligibility information when its service provider acting on its behalf receives such information.
4. *Constructive sharing.* The rule does not prohibit a person and its affiliate from engaging in “constructive sharing” of eligibility information for use in marketing solicitations to consumers when the affiliate making the solicitations has a pre-existing business relationship with the consumer, so long as the rule’s restrictions on the use of eligibility information are met. In general, “constructive sharing” refers to the ability of a person to benefit from its affiliate’s eligibility information for use in marketing as long as the person does not actually receive or use the information.
- a. Thus, a person may use its own eligibility information to market an affiliate’s products and services to that person’s customers, so long as the affiliate does not use the person’s eligibility information to identify the recipients of the solicitation, to establish criteria used to select recipients of the solicitation or to decide which products or services to market. In other words, this means that the affiliate cannot use the person’s eligibility information to “make solicitations” as that term is described above.
 - b. The rule also permits constructive sharing if, in the above situation, the person directs its service provider to market the affiliate’s products or services to that person’s customers, as long as the above conditions are met and the affiliate

does not communicate directly with the service provider regarding the use of the eligibility information.

5. *Use of service providers that maintain or access common databases to market under the constructive sharing rules.*
 - a. A service provider that maintains or accesses a common database may use one affiliate's eligibility information to market another affiliate's products or services to the first affiliate's customers under the constructive sharing rules, so long as –
 - i. the first affiliate on whose behalf the service provider acts –
 - controls access to and use of its eligibility information by the service provider (including the right to establish the specific terms and conditions under which the service provider may use the information to market the products or services);
 - establishes specific terms and conditions under which the service provider may access and use the first affiliate's eligibility information to market the products and services (or those of affiliates generally) to the consumer,
 - periodically evaluates the service provider's compliance with those terms and conditions; and
 - requires the service provider to implement reasonable policies and procedures designed to ensure that the service provider uses the affiliate's eligibility information in accordance with the terms and conditions;
 - ii. The first affiliate (whose consumers' eligibility information is used) is identified on or with the marketing materials provided to the consumer; and
 - iii. The second affiliate does not use the first affiliate's eligibility information to identify the recipients of the solicitation, to establish criteria used to select recipients of the solicitation or to decide which products or services to market.
 - b. *Written requirements.* The above requirements between the first affiliate and the service provider must be in writing, and the specific terms and conditions established by the first affiliate above must be set forth in writing.

D. Exceptions

1. The rule does not apply to the use of eligibility information to –
 - a. make a solicitation for marketing purposes to a consumer with whom the affiliate using the eligibility information has a pre-existing business relationship;

- b. facilitate communications to an individual for whose benefit the person using the information provides employee benefit or other services pursuant to a contract with an employer related to and arising out of a current employment relationship or status of the individual as a participant or beneficiary of an employee benefit plan;
 - c. perform services on behalf of an affiliate, as long as the affiliate would not be prohibited by the rule from engaging in the services on its own behalf;
 - d. respond to a communication about the person's products or services initiated by the consumer; or
 - e. respond to an authorization or request by the consumer to receive solicitations.
2. The rule also does not apply to a person's use of eligibility information received from an affiliate if compliance with the rule would prevent the person from complying with its state insurance law pertaining to unfair discrimination.

E. Scope and Duration of Opt-out

1. *Scope of Opt Out.* The scope may depend upon whether the consumer establishes a continuing relationship with the person or its affiliate or enters into an isolated transaction.
 - a. *For continuing relationships,* the opt-out notice may apply to all current and potential future relationships and transactions, as long as the notice describes the relationships and transactions covered by the opt-out. Examples of activities that establish a continuing relationship with an affiliate include when the consumer opens a credit account, obtains a loan, purchases an insurance product, holds an investment product, enters into a home mortgage broker agreement, leases personal property or obtains a financial, investment or economic advisory services.
 - b. *For isolated transactions,* with no continuing relationship, the opt-out notice may apply only to eligibility information obtained in connection with that transaction. Examples of isolated transactions include when the consumer withdraws cash from an ATM or purchases a money order, airline tickets, travel insurance or travelers checks.
2. *Menu of alternatives.* As long as a consumer may opt out of all solicitations from all affiliates, the consumer may also be given the opportunity to choose from a menu of opt-out alternatives, such as by electing to –
 - a. opt out of solicitations from certain types of affiliates,

- b. opt out of solicitations based on only certain types of eligibility information, or
 - c. opt out of solicitations by only certain methods of delivery.
3. *Notice and opt-out notice requirements after termination of all continuing relationships.*
- a. If after termination of all continuing relationships, the consumer subsequently establishes another continuing relationship with the person or its affiliates and the consumer's eligibility information is to be used to make a solicitation, then the consumer must be give an new notice and opt-out.
 - b. The new opt-out notice must apply, at a minimum, to eligibility information obtained in connection with the new continuing relationship.
 - c. The consumer's decision not to opt out after receiving the new opt-out notice does not override a prior opt-out with respect to eligibility information obtained in connection with a terminated relationship.
4. *Duration of Opt-out.* The opt-out period must be at least five years, but may last unless revoked by the consumer.
5. *Time of Opt-out.* A consumer may opt out at any time.

F. Contents of Opt-Out Notice

- 1. The notice must be "clear, conspicuous and concise" and must disclose –
 - a. The names of the affiliate(s) providing the notice.
 - If the notice is provided jointly by multiple affiliates that share a common name (e.g., "ABC") the notice may indicate that it is provided by multiple companies with the ABC name or multiple companies in the ABC group or family of companies, such as by indicating that the notice is provided by "all of the ABC companies," "the ABC banking, credit card, insurance, and securities companies," or by listing the name of each affiliate providing the notice.
 - If the affiliates providing the joint notice do not all share a common name, the notice must either separately identify each affiliate by name or identify each of the common names used by the affiliates (e.g., the notice is provided by "all of the ABC and XYZ companies" or by "the ABC banking and credit card companies and the XYZ insurance companies").

- b. A list of the affiliates or types of affiliates whose use of eligibility information is covered by the notice, which may include companies that become affiliates after the notice is provided to the consumer.
- If each affiliate shares a common name (such as “ABC”) the notice may indicate that it applies to multiple companies with the ABC name or multiple companies in the ABC group or family of companies, such as by stating that the notice is provided by “all of the ABC companies,” “the ABC banking, credit card, insurance, and securities companies,” or by listing the name of each affiliate providing the notice.
 - If the affiliates providing the notice do not all share a common name, the notice must either separately identify each covered affiliate by name or identify each of the common names used by those affiliates, for example, by stating that the notice applies to “all of the ABC and XYZ companies” or to “the ABC banking and credit card companies and the XYZ insurance companies.”
- c. A general description of the types of eligibility information that may be used to make solicitations to the consumer.
- d. That the consumer may opt out of the use of eligibility information to make solicitations;
- e. That the consumer’s opt-out will apply for the specified period of time stated in the notice and, if applicable, that the consumer will be allowed to renew the election once that period expires.
- f. If the notice is provided to consumers who may have previously opted out (such as if an annual notice), that a consumer who has opted out need not act again until she receives a renewal notice; and
- g. A reasonable and simple method for the consumer to opt out.

2. *Joint relationships.*

- a. A single opt-out notice may be provided to joint consumers, and any joint consumer may opt-out.
- b. The opt-out notice must explain how an opt-out by a joint consumer will be treated.
- An opt-out by a joint consumer may apply to all the joint consumers, or
 - Each joint consumer may be permitted to opt out separately. If each joint consumer is permitted to opt out separately, one joint consumer must be

permitted to opt out on behalf of all of the joint consumers and the joint consumers must be permitted to exercise their separate rights to opt out in a single response.

- c. It is impermissible to require all joint consumers to opt out before implementing any opt-out direction.
3. *Alternative contents.* If the consumer has a broader opt-out right than the rule requires, the consumer may be given a clear, conspicuous, and concise notice that accurately discloses the opt-out rights.
4. *Coordinated and consolidated notices.* Any person subject to the rule may provide the affiliate marketing notice along with GLBA privacy notices or any other required notice.
5. *Equivalent notices.* A notice or other disclosure that is equivalent to the affiliate marketing notice and that is provided to a consumer together with disclosures required by any other provision of law, satisfies the affiliate marketing rule.

G. Reasonable Opportunity to Opt-out

1. Consumer must be given a “reasonable opportunity to opt out.”
2. Examples of reasonable opportunity to opt out –
 - a. By mail and the consumer is given 30 days from the date the notice is mailed to elect to opt out by any reasonable means.
 - b. By electronic means, such as by posting the notice at an Internet Web site where the consumer obtains a product or service. Reasonable opportunity to opt out by electronic means should provide for the following:
 - The consumer acknowledges receipt of the electronic notice.
 - The consumer is given 30 days to opt-out by any reasonable means.
 - The opt-out notice is provided to the consumer by e-mail where the consumer has agreed to receive disclosures by e-mail.
 - The consumer is given 30 days after the e-mail is sent to opt out by any reasonable means.
 - c. At the time of an electronic transaction, such as a transaction conducted on an Internet Web site.
 - The opt-out notice is provided to the consumer at the time of the electronic transaction.
 - The consumer is required to decide, as a necessary part of proceeding with the transaction, whether to opt out before completing the transaction.
 - There is a simple process that the consumer may use to opt out at that time using the same mechanism through which the transaction is conducted.

- d. At the time of an in-person transaction.
 - The opt-out notice is provided to the consumer in writing at the time of the transaction.
 - The consumer is required to decide, as a necessary part of proceeding with the transaction, whether to opt out before completing the transaction, and is not permitted to complete the transaction without making a choice. There is a simple process, such as completing a form that requires the consumer to write a “yes” or “no,” or to check one of two blank check boxes.
- e. The opt-out notice is included in a GLBA privacy notice.
 - The consumer must have the opportunity to opt out within a reasonable period of time and in the same manner as the opt-out under that privacy notice.

H. Reasonable and Simple Methods of Opting Out

1. Consumers must be provided a reasonable and simple method to opt out.
2. Reasonable and simple methods for exercising the opt-out right include –
 - a. Designating a check-off box in a prominent position on the opt-out form;
 - b. Including a reply form and a self-addressed envelope with the opt-out notice;
 - c. Providing an electronic means to opt out, such as a form that is electronically mailed or processed at an Internet Web site, if the consumer agrees to the electronic delivery of information;
 - d. Providing a toll-free telephone number to receive opt-out requests; or
 - e. Allowing consumers to exercise all of their opt-out rights described in a consolidated opt-out notice that includes the GLBA privacy opt-out, the FCRA affiliate sharing opt-out, and the FCRA affiliate marketing opt-out, by a single method, such as by calling a single toll-free telephone number.
3. Reasonable and simple methods for exercising an opt-out right do not include –
 - a. Requiring the consumer to write his or her own letter;
 - b. Requiring the consumer to call or write to obtain a form for opting out, rather than including the form with the opt-out notice;
 - c. Requiring the consumer who receives the opt-out notice in electronic form

only, such as through posting at an Internet Web site, to opt out solely by paper mail or by visiting a different Web site without providing a link to that site.

4. *Specific opt-out means.* Each consumer may be required to opt out through a specific means, as long as that means is reasonable and simple for that consumer.

I. Delivery of Opt-Out Notice

1. The opt-out notice must be provided so that each consumer can reasonably be expected to receive actual notice.
2. Opt-out notices may be provided electronically in compliance with either the rule's electronic disclosure provisions or E-SIGN.
3. *Examples of reasonable expectation of actual notice.* A consumer may reasonably be expected to receive actual notice if the affiliate providing the notice:
 - a. Hand-delivers a printed copy of the notice to the consumer;
 - b. Mails a printed copy of the notice to the consumer's last known mailing address.
 - c. Provides a notice by e-mail to a consumer who has agreed to receive electronic disclosures by e-mail from the affiliate providing the notice; or
 - d. Posts the notice on the Internet Web site at which the consumer obtained a product or service electronically and requires the consumer to acknowledge receipt of the notice.
4. *Examples of no reasonable expectation of actual notice.* A consumer may not reasonably be expected to receive actual notice if the affiliate providing the notice:
 - a. Only posts the notice on a sign in a branch or office or generally publishes the notice in a newspaper;
 - b. Sends the notice via e-mail to a consumer who has not agreed to receive electronic disclosures by e-mail from the affiliate providing the notice; or
 - c. Posts the notice on an Internet Web site without requiring the consumer to acknowledge receipt of the notice.

J. Renewal of Opt-Out

1. Each opt-out renewal must be effective at least five years.
2. After an opt-out period expires, an affiliate may not make marketing solicitations covered by the rule to consumers who have opted out unless an exception applies or the targeted consumers have been given a renewal notice with a reasonable and simple method to renew the opt-out, and have not renewed the opt-out.
3. Renewal notices must be provided either by the affiliate that provided the previous opt-out notices or as part of a joint renewal notice from the affiliates that jointly provided the previous opt-out notices.
4. The renewal notice must be clear, conspicuous, and concise, and must accurately disclose—
 - a. The names of the affiliate(s) providing the notice.
 - If the notice is provided jointly by multiple affiliates that share a common name (e.g., “ABC”) the notice may indicate that it is provided by multiple companies with the ABC name or multiple companies in the ABC group or family of companies, such as by indicating that the notice is provided by “all of the ABC companies,” “the ABC banking, credit card, insurance, and securities companies,” or by listing the name of each affiliate providing the notice.
 - If the affiliates providing the joint notice do not all share a common name, the notice must either separately identify each affiliate by name or identify each of the common names used by the affiliates (e.g., the notice is provided by “all of the ABC and XYZ companies” or by “the ABC banking and credit card companies and the XYZ insurance companies”).
 - b. A list of the affiliates or types of affiliates whose use of eligibility information is covered by the notice, which may include companies that become affiliates after the notice is provided to the consumer.
 - If each affiliate shares a common name (such as “ABC”) the notice may indicate that it applies to multiple companies with the ABC name or multiple companies in the ABC group or family of companies, such as by stating that the notice is provided by “all of the ABC companies,” “the ABC banking, credit card, insurance, and securities companies,” or by listing the name of each affiliate providing the notice.
 - If the affiliates providing the notice do not all share a common name, the notice must either separately identify each covered affiliate by name or identify each of the common names used by those affiliates, for example,

by stating that the notice applies to “all of the ABC and XYZ companies” or to “the ABC banking and credit card companies and the XYZ insurance companies.”

- c. A general description of the types of eligibility information that may be used to make solicitations to the consumer.
 - d. That the consumer previously opted out of the use of eligibility information to make solicitations;
 - e. That the consumer’s opt-out has expired or is about to expire;
 - f. That the consumer may renew the opt-out;
 - g. If applicable, that the consumer’s election to renew will apply for the specified period of time stated in the notice and that the consumer will be allowed to renew the election once that period expires; and
 - h. A reasonable and simple method for the consumer to opt out.
5. *Timing* – A renewal notice may be provided to the consumer either—
- a. A reasonable period of time before the opt-out period expires; or
 - b. Any time after the opt-out period expires but before making solicitations that would have been prohibited by the expired opt-out period.

Providing the renewal notice with the annual GLBA privacy notice before expiration of the opt-out period is a reasonable period of time before expiration of the opt-out.

- 6. An opt-out period may not be shortened by sending a renewal notice to the consumer before expiration of the opt-out period, even if the consumer does not renew the opt-out.

J. Prospective Application

- 1. Affiliates may use eligibility information received from an affiliate to make solicitations to a consumer if the information is received prior to October 1, 2008.
- 2. An affiliate is deemed to receive eligibility information when the information is placed into a common database and is accessible by the affiliates.

K. Model Notices

An appendix to each of the Federal Agencies' versions of the affiliate marketing rule provides model forms for the required opt-out notices.

Red Flag Rules – Compliance Issues
Anne P. Fortney
Hudson Cook, LLP

I. Overview

The Fair and Accurate Credit Transactions Act (“FACT Act”) amended the Fair Credit Reporting Act (“FCRA”) by requiring the federal banking agencies, the National Credit Union Administration, and the Federal Trade Commission (“Federal Agencies”) to adopt rules and guidelines for covered entities to implement in order to detect, prevent and mitigate identity theft (“*red flag rules*”).¹

The Federal Agencies published proposed *red flag rules and guidelines* in July, 2006. Following a public comment period, the Federal Agencies published the final rules and guidelines in the Federal Register in November, 2007.² *Compliance with the red flags rule and guidelines became mandatory on November 1, 2008; however the FTC will forebear enforcement as to entities under its jurisdiction until May 1, 2009.*

The red flags rule requires a covered financial institution or creditor (“covered entity”) subject to the rule to develop and implement a written *Identity Theft Prevention Program (“Program”)*. The Program must be designed to detect, prevent, and mitigate identity theft, and must be appropriate to the size and complexity of the covered entity and the nature and scope of the entity’s activities.

The Program must include reasonable policies and procedures to identify, detect and respond to “red flags.” A red flag is “a pattern, practice, or specific activity that indicates the possible existence of identity theft.”³ A covered entity must also update the Program periodically to (1) determine whether its Program reaches all accounts satisfying the rule’s definition of “covered account” and (2) ensure that the Program, including identified red flags, is updated periodically to reflect changes in risk of identity theft.

In the administration of the Program, the entity must obtain approval for the initial Program from senior management; involve senior management in the oversight, development, implementation, and administration of the Program; train staff to effectively administer the Program; and exercise appropriate and effective oversight of service provider arrangements.

Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A to the Rule and include in its Program those guidelines that are appropriate. Although the guidelines consist of a list of compliance suggestions, with examples, a covered entity’s *consideration of the guidelines is mandatory, not optional*. Covered entities must review the guidelines and apply them to their Program as appropriate.

¹ FACT Act §114.

² 72 Fed. Reg. 63718 (Nov. 9, 2007).

³ “Identity theft” is defined as “a fraud committed or attempted using the identifying information of another person without authority.” 16 C.F.R. §§ 681.2(b)(8); 603.2(a).

II. Background for Discussion of Compliance Issues

A. **Scope** – Apply to “financial institutions and creditors” that are within the respective jurisdictions of the OCC, FRB, FDIC, OTS, NCUA and FTC.

1. Scope includes financial institutions and creditors that subject to administrative enforcement of the FCRA by the Federal Trade Commission under FCRA section 621(a).
2. Does not include brokers, dealers, insurance companies, investment companies or investment advisers.

B. Definitions

1. *Financial Institution* – means 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 (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer.
2. *Creditor and Credit* – same as the ECOA definitions
 - a. Creditor means “any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit.”
 - b. Credit means “the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefor.”
 - c. Definition includes hospitals, universities, utilities, as well as “traditional” creditors.
 - d. Also includes third-party debt collectors who regularly arrange for the extension, renewal or continuation of credit.
3. *Account*
 - a. Definition: An “account” means “continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.”
 - b. The Federal Agencies intend the definition of account to include “a relationship with a creditor, such as an automobile dealer or a

telecommunications provider, primarily to obtain a product or service that is not financial in nature.”

4. *Covered Account*

- a. A “covered account” means “an account that the creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions AND any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.”

5. *Service Provider* -- means a person that provides a service directly to the financial institution or creditor.

C. Periodic Identification of Covered Accounts. Each financial institution or creditor must periodically conduct a risk assessment to determine whether it offers or maintains “covered accounts,” taking into consideration:

1. The methods it provides to open its accounts;
2. The methods it provides to access its accounts; and
3. Its previous experiences with identity theft.

D. Establishment of an Identity Theft Prevention Program.

1. *Program requirement.* Each financial institution or creditor that offers or maintains one or more “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. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.
2. *Elements of the Program.* The Program must include reasonable policies and procedures to:
 - A. Identify relevant Red Flags for the covered accounts and incorporate those Red Flags into the Program;
 - B. Detect Red Flags that have been incorporated into the Program;
 - C. Respond appropriately to any Red Flags that are detected; and

- D. Ensure the Program (including any relevant Red Flags) is updated periodically, to reflect changes in identity theft risks to customers and to the safety and soundness of the financial institution or creditor.
3. *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:
- A. Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;
 - B. Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;
 - C. Train staff, as necessary, to effectively implement the Program; and
 - D. Exercise appropriate and effective oversight of service provider arrangements.
4. *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the Guidelines and include in its Program those guidelines that are appropriate.

Appendix A

Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

The federal agencies developed the following guidelines to assist financial institutions and creditors in the formulation and maintenance of an Identity Theft Prevention Program under the Red Flags Rules.

I. The Program. In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

- (1) The types of covered accounts it offers or maintains;
- (2) The methods it provides to open its covered accounts;
- (3) The methods it provides to access its covered accounts; and
- (4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

- (1) Incidents of identity theft that the financial institution or creditor has experienced;
- (2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
- (3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.

- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- (2) The presentation of suspicious documents;
- (3) The presentation of suspicious personal identifying information, such as a suspicious address change;
- (4) The unusual use of, or other suspicious activity related to, a covered account; and
- (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags. The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft. The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

- (b) Contacting the customer;
- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
- (d) Reopening a covered account with a new account number;
- (e) Not opening a new covered account;
- (f) Closing an existing covered account;
- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement; or
- (i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program. Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

- (a) The experiences of the financial institution or creditor with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft;
- (d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and
- (e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program.

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

- (1) Assigning specific responsibility for the Program's implementation;
- (2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and
- (3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.*

- (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with the Red Flags Rules.
- (2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of

identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

- (c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements. Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

- (a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;
- (b) Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;
- (c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and
- (d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix A, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries;
 - b. An unusual number of recently established credit relationships;
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
 - a. The address does not match any address in the consumer report; or
 - b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- a. The address on an application is the same as the address provided on a fraudulent application; or
- b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- a. The address on an application is fictitious, a mail drop, or a prison; or
- b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

- a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
- b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- a. Nonpayment when there is no history of late or missed payments;
- b. A material increase in the use of available credit;
- c. A material change in purchasing or spending patterns;
- d. A material change in electronic fund transfer patterns in connection with a deposit account; or
- e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

**ABA – Consumer Financial Services Committee
2008 Winter Meeting
Summary of Red Flags, Address Discrepancy and Affiliate Sharing Rules**

Red Flags Rule:

- On November 9, 2007, the Banking Agencies, the National Credit Union Administration (“NCUA”) and the Federal Trade Commission (“FTC”) published a joint final rule and guidelines to implement the red flag requirements of the Fair Credit Reporting Act (“FCRA”). The red flags rule took effect on January 1, 2008; compliance, however, was not required until November 1, 2008. The FTC suspended its enforcement of the rule until May 1, 2009 for entities subject to FTC oversight.
- The red flags rule requires each “financial institution” or “creditor” to establish an Identity Theft Prevention Program (“Program”) to detect, prevent and mitigate identity theft in connection with accounts that are “covered accounts” within the meaning of the rule.
 - “Financial institution” is defined to mean a person that holds a “transaction account” belonging to a consumer.
 - “Creditor” has the same meaning as in the Equal Credit Opportunity Act (“ECOA”)—*i.e.*, ECOA/Regulation B defines creditor to mean “any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit.” Credit is defined as “the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefor.”
- The red flags rule requires that an institution, initially and periodically thereafter, conduct a risk assessment to determine whether it “offers or maintains any covered accounts.” “Account” is defined as “a continuing relationship.” An isolated event, such as the purchase of a cashier’s check or money order, therefore is not a “covered account.” In addition, an institution must incorporate into its Program reasonable policies and procedures to detect red flags.

Address Discrepancies:

- The address discrepancy rule also imposes certain address verification and confirmation requirements on a user of a consumer report that receives a “notice of address discrepancy” from a consumer reporting agency.
- “Notice of address discrepancy” is defined as “a notice sent to a user by a consumer reporting agency . . . that informs the user of a substantial difference between the address for the consumer that the user provided to the [consumer reporting agency] and the address(es) in the [consumer reporting agency’s] file for the consumer.”

- Verification Requirement. The address discrepancy rule requires that a user “develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.”
- In certain specific circumstances, the rule requires that a user furnish a verified address to a consumer reporting agency.

Affiliate Marketing Rule:

- In October and November, 2007, the banking agencies, the NCUA and the FTC published final rules to implement the affiliate marketing requirements of section 624 of the FCRA.
- An institution may not use “eligibility information” relating to a consumer that the institution receives from an affiliate “to make a solicitation for marketing purposes to the consumer” unless:
 - It is “clearly and conspicuously” disclosed to the consumer that the institution may use eligibility information received from an affiliate to make marketing solicitations to the consumer;
 - The consumer is provided a reasonable opportunity to opt out; and
 - The consumer has not opted out.
- The rule defines “eligibility information” as “any information the communication of which would be a consumer report if exclusions from the definition of ‘consumer report’ in section 603(d)(2)(A) of the [FCRA] did not apply.”