

SUBJECT: Fair Credit Reporting Act

INTRODUCTION.....	1	Duties When Notified by CRA of Consumer's Dispute	9
EXECUTIVE SUMMARY	1	DUTY TO REPORT VOLUNTARY CLOSING OF CREDIT ACCOUNT ..	10
FACT ACT CHANGES.....	2	DUTY TO REPORT DATES OF DELINQUENCIES.....	10
DEFINITIONS	2	LIABILITY FOR VIOLATIONS OF THE FCRA	10
Compliance Tip	3	WISCONSIN SECURITY FREEZE LAW	10
PERMISSIBLE PURPOSES OF CONSUMER REPORTS	4	REPORTING AFTER ERROR NOTICE ON MORTGAGE LOANS	11
USING CONSUMER REPORTS FOR EMPLOYMENT PURPOSES	4	EXHIBIT A – DEPOSIT ACCOUNT ADVERSE ACTION NOTICE	
Investigating Suspected Employee Misconduct.....	5	BASED ON CONSUMER REPORT	12
USING INVESTIGATIVE CONSUMER REPORTS	5	EXHIBIT B – GUIDE TO THE FACT ACT.....	13
MEDICAL INFORMATION	5	EXHIBIT B1 – Model Form for Initial Opt-out notice (Single-Affiliate	
Limitation on Creditors.....	6	Notice)	58
ADVERSE ACTION NOTICES.....	6	EXHIBIT B2 – Model Form for Initial Opt-out notice (Joint Notice).....	59
IDENTITY THEFT	7	EXHIBIT B3 – Model Form for Renewal Notice (Single-Affiliate	
Making Information Available to Victims	7	Notice)	60
USING “PRESCREENED LISTS”.....	7	EXHIBIT B4 – Model Form for Renewal Notice (Joint Notice)	61
DUTY TO FURNISH ACCURATE INFORMATION.....	9	EXHIBIT B5 – Model Form for Voluntary “No Marketing” Notice.....	62
Duties When Notified by Consumer.....	9		

INTRODUCTION

This release applies to all credit unions, state and federal. It describes the federal Fair Credit Reporting Act (FCRA). The FCRA affects credit unions in regard to member accounts, employment, lending decisions, and protection of members from fraud and identity theft.

EXECUTIVE SUMMARY

To obtain a consumer report (such as a credit report or account reporting service) a credit union must certify to the Consumer Reporting Agency that the report will be used only for a “permitted purpose,” such as:

- For the extension of credit as a result of an application from a consumer;
- For the review or collection of a consumer's account;
- When there is a legitimate business need in connection with a business transaction that is initiated by the consumer; and
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account.

A consumer report may only be obtained for employment purposes if the consumer is provided a special disclosure and gives their written consent. If the credit union intends to take adverse action on employment, based on the consumer report, it must first give the consumer a copy of the credit report and a summary of consumer rights. Later, upon taking the adverse action, the credit union must provide an adverse action notice. Credit unions, in their capacities as employers, cannot discriminate on the basis of bankruptcy.

Special rules apply to investigations of suspected employee misconduct by outside parties. Employees need not be given prior notice of such investigations, if certain conditions are met.

The FCRA definition of adverse action requires a “denial” notice when turning down a request to open a share, share draft, or other member account at the credit union if the decision is based in whole or in part on information from a consumer report.

Please note that Reg. B imposes additional requirements for adverse actions when related to credit transactions.

The FCRA requires that adverse action (denial) notices contain:

- The telephone number of the consumer reporting agency;
- A statement that the CRA did not make the adverse action decision;

- A statement of the consumer's right to a free credit report if requested within 60 days; and
- The consumer's right to dispute information in the report.

Language for these disclosures is included in The League's Reg. B denial form (#82029), for credit transactions. A different form, such as The League's Deposit Account Adverse Action Notice Based on Consumer Report (#82058), shown in Exhibit A, may be used in connection with member accounts.

Parts of the FCRA are designed to help fight identity theft. As of June 1, 2004, if a credit union does business with an identity thief, it will have to provide a copy of any application or transaction records it has to the victim or to police, upon request. Credit unions have duties to furnish accurate information, investigate disputed information, and notify credit reporting agencies of disputed information.

The FCRA restricts prescreened credit offers. Consumers given such offers must be given a notice stating that a consumer report was used and how the consumer may prohibit future prescreening.

This release also describes how Wisconsin consumers can have a security freeze placed on their credit reports. The security freeze, in effect, "locks" the individual's credit report and credit score from being released to extend credit unless the individual specifically authorizes it. The security freeze law does not apply to information the credit union may request with respect to a person's existing accounts or contracts with the credit union. It also does not apply to anyone with a legitimate business need for the information in connection with a business transaction initiated by the individual.

FACT ACT CHANGES

On December 4, 2003, President Bush signed the Fair and Accurate Credit Transactions Act, the "FACT Act," which makes some important changes in the Fair Credit Reporting Act. Some of those changes have already gone into effect, and others will become effective in the future as the financial institution regulators, including NCUA, issue new rules.

Until all of the regulations are final, credit unions face a confusing array of new rules with different effective dates. Exhibit C to this release is the "WCUL Guide to the FACT Act," which summarizes all the FCRA changes. The Guide's information is organized in order of its current significance to credit unions. Those new requirements that need your immediate attention are listed first. Less significant requirements or those awaiting implementing regulations are listed later. Eventually, all of the Guide material will be added to the main body of this release.

Here are some of the more significant FACT Act changes:

- Requiring mortgage lenders to disclose credit scores to applicants, along with a notice explaining the score;
- Requiring that consumers be notified when negative information is reported to a credit reporting agency (CRA);
- Allowing consumers to block ID theft information from appearing on credit reports, either by notifying the CRA or by notifying the credit union directly;
- Prohibiting credit unions from "re-polluting" credit reports, i.e., re-furnishing information based on ID-theft-related information;
- Prohibiting credit unions from selling, transferring or collecting on any debt caused by ID theft;
- Requiring certain precautions before credit unions can extend credit to consumers who have placed fraud alerts or active duty alerts on their credit reports;
- Requiring new document disposal policies;
- Giving consumers enhanced rights to opt-out of prescreened credit offers or to prohibit credit unions with sharing consumer information with affiliates (like CUSOs) for marketing purposes;
- Requiring credit unions that use risk-based lending to give notices to consumers who get credit on less-favorable terms than other borrowers;
- Requiring credit unions to reinvestigate disputed information upon request directly from a consumer;
- Requiring credit unions to reconcile potentially fraudulent consumer address information; and
- Requiring credit unions to develop policies and procedures to uncover identity theft.

DEFINITIONS

Active Duty Military Consumer: A consumer in full-time U.S. military service who is on active duty (including training), or a reservist called to active full-time duty. This definition only applies to those assigned to service away from their usual duty station. This FCRA definition differs from similar terms used in the Servicemembers Civil Relief Act. See ii Release No. 0072 for information on the SCRA.

Adverse Action: Includes the following actions relating to credit unions (or CUSOs):

- A denial or revocation of credit, an adverse change in terms of existing credit, or a refusal to grant credit on substantially the same terms as requested;
- A denial of employment, or any other employment decision that adversely affects an existing or prospective employee;
- An action that is adverse to the interests of the consumer in connection with an application or review of an account of any type; and
- A denial or cancellation of insurance or other adverse change in connection with insurance that is existing or applied for. FCRA § 603(k).

Consumer Report: Information (such as a credit report, driver's license record, or account reporting service) provided by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, which is to be used as a factor in establishing the consumer's eligibility for credit, insurance, or employment purposes.

However, the term does not include providing such information if it is based solely on transactions or experiences between the consumer and person making the report, or communication of that information among persons related by common ownership or affiliated by corporate control.

Thus, a credit union may take information solely relating to its own experiences with a member and share that information with its CUSO, and vice versa. However, this sharing does not extend to information that relates to the experiences of third parties with the member (e.g., credit reports or other third party verifications). That information may only be shared with a CUSO or other affiliate if the member is given a clear and conspicuous disclosure that the information may be shared between the affiliates *and* the member is given the opportunity, before the information is shared, to direct that the information not be shared

The NCUA's rules require this disclosure to be included in the credit union's privacy disclosures. See *ii Release No. 0152*, which includes an exhibit showing NCUA's sample disclosure for this purpose.

Consumer Reporting Agency (CRA): A person or organization regularly engaged in the practice of assembling or evaluating consumer credit or other information for the purpose of furnishing consumer reports to third parties. The typical example is a credit bureau, but others are account or check verification services (ChexSystems, Accucheck, Telecheck), and tenant verification services. § 603(f).

Fraud Alert / Active Duty Alert: A clear and conspicuous statement that notifies users of a consumer report that the consumer may be a victim of fraud or identity theft, or that the consumer is an active duty military consumer.

Identity Theft: A fraud committed using the identifying information of another person.

Identity Theft Report: A copy of a report alleging identity theft that has been filed with a law enforcement agency.

Investigative Consumer Report: A consumer report in which the consumer information is, in whole or in part, obtained through personal interviews with neighbors, friends, associates or others of the consumer's acquaintance, other than information obtained from the consumer or the consumer's creditors. § 603(e).

Medical Information: Information about a consumer's past, present or behavioral health, the health care that has been provided to a consumer, or payments for health care. It does not include age, gender, or demographic information about a consumer, or any other information not related to health, such as the existence or value of an insurance policy.

Prescreening: Though not specifically defined in the FCRA, prescreening typically involves asking a consumer reporting agency to provide a list of consumers who meet certain criteria for creditworthiness.

Compliance Tip

Credit unions should take care never to pass on member information to third parties that was not based solely on the credit union's own experience with the member. Doing so may constitute a consumer report, and subject the credit union to the additional compliance requirements of a consumer reporting agency. High risk practices include sharing information from any of the following with other credit unions, banks, collectors, or other third parties:

- Credit reports,
- Account verification service reports,
- Member's credit references or credit history on loan applications,
- Informal "bad check or account closed" lists based on other institutions' experiences.

PERMISSIBLE PURPOSES OF CONSUMER REPORTS

The FCRA limits the use of consumer reports to protect consumers' privacy. Therefore, credit unions and others that use consumer reports must have a "permissible purpose" to obtain them under the FCRA. Consumer reports may be lawfully obtained under the following circumstances and no other:

- (1) In response to the order of a court having jurisdiction, or a subpoena issued in connection with proceedings before a federal grand jury;
- (2) *In accordance with the written instructions of the consumer to whom it relates;*
- (3) To a person which the consumer reporting agency has reason to believe:
 - (A) *intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer;*
 - (B) *intends to use the information for employment purposes, including hiring and promotion decisions, where the consumer has given written permission* (see the section on "Using Consumer Reports for Employment Purposes, later in this ii Release);
 - (C) *intends to use the information in connection with the underwriting of insurance involving the consumer;*
 - (D) *intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status;*
 - (E) *intends to use the information, as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation;*
 - (F) *otherwise has a legitimate business need for the information*
 - (i) *in connection with a business transaction that is initiated by the consumer; or*
 - (ii) *to review an account to determine whether the consumer continues to meet the terms of the account.*
 - (G) *executive departments and agencies in connection with the issuance of government-sponsored individually-billed travel charge cards.*

Creditors and insurers may also obtain certain consumer report information for the purpose of making "*prescreened*" *unsolicited credit offers*. (See the section titled *Duties of Credit Unions Using "Prescreened Lists,"* later in this release.)

The FCRA prohibits anyone from obtaining a consumer report from a CRA unless the person has certified to the CRA the permissible purpose for obtaining the report and certifies that it will not be used for any other purpose.

USING CONSUMER REPORTS FOR EMPLOYMENT PURPOSES

If a credit union obtains a consumer report for employment decisions (such as hiring or promotion decisions) it must:

- Provide a clear and conspicuous written disclosure to the consumer before obtaining the report, in a document that consists *only* of the disclosure, stating that the credit union may obtain a consumer report for employment purposes;
- Obtain written permission of the consumer before obtaining the report; and
- Provide a certification to the CRA that: (1) the information obtained will not be used in violation of any federal or state equal opportunity law or regulation, (2) it has provided proper disclosure to the consumer, and (3) if any adverse action is to be taken based on the consumer report, the credit union will provide the consumer with a copy of the consumer report and a summary of the consumer's rights (before taking the adverse action). § 604(b).

Also, an adverse action notice is required if any such action is taken, based in whole or in part on the consumer report. Even before the adverse action is taken, however, the credit union must provide the employee/applicant with a copy of the consumer report and the Summary of Consumer Rights (obtained from the CRA). See "Adverse Action Notices" later in this release.

It is important to remember that the Bankruptcy Code prohibits employers from discriminating on the basis of bankruptcy.

Investigating Suspected Employee Misconduct

Employers using outside parties to investigate workplace misconduct do not have to provide advance notice to an employee, or get his/her consent, or disclose the contents of the investigator's report before taking adverse action.

Because of FACT Act amendments to the FCRA, investigative reports of suspected employee misconduct are not within the FCRA's definition of a consumer report / investigative consumer report. As a result, an employer can use a third party to conduct a workplace investigation without following the FCRA consent and disclosure requirements. (Before March 31, 2004, the Federal Trade Commission required employers to get an employee's consent before the third party investigation, essentially "tipping off" the employee.)

To qualify for this exemption, the report:

- Must involve suspected misconduct, a violation of law or regulations, or a violation of the employer's written policies;
- Must not be provided to any person except the employer or its agent, the government, or as required by law; and
- Must not be made for the purpose of investigating creditworthiness.

If "adverse action" is taken against the employee based in whole or in part on the results of the investigation, the employer must give the employee a summary of the nature and substance of the report. "Adverse action" means any employment decision that adversely affects an employee. So, employers using outside parties to conduct internal investigations must provide this summary, even if the only adverse action taken is a written warning. Sources of information, such as the identities of people interviewed, need not be disclosed in the summary.

Nothing in the FACT Act changes an employer's obligation under the FCRA to give notice to and obtain the prior consent of job applicants or current employees when it wishes to use an outside firm to conduct a background check. §603(x).

USING INVESTIGATIVE CONSUMER REPORTS

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews.

If the credit union intends to obtain an investigative consumer report, it must provide a written disclosure to the consumer, mailed or delivered no more than three days after the date the report was ordered. The disclosure must state:

- That the credit union may obtain an investigative consumer report;
- That the consumer has the right to request additional disclosures of the nature and scope of the investigation (described below); and
- A Summary of Consumer Rights (this will be provided to the credit union by the CRA).

If the consumer, within a reasonable period of time after receiving the above disclosures, makes a written request, the credit union must make a complete disclosure of the nature and scope of the investigation that was requested. This must be in a written statement that is mailed or delivered to the consumer no more than five days after the later of (1) receiving the consumer's request for the information, or (2) when the report was first requested. § 606.

MEDICAL INFORMATION

As of June 1, 2004, a CRA generally may not provide medical information about a consumer unless:

- The report is for an insurance transaction and the consumer consents;
- The report is for employment purposes or a credit transaction, and the consumer provides specific written consent, describing in clear and conspicuous language the use for which the information will be furnished; or
- The information (other than account status or amounts) pertains solely to debts arising from the receipt of medical services or products. § 604(g).

Those who receive medical information may not disclose it (even to share with an affiliate) for any reason other than to carry out the purpose for which it was disclosed, or as otherwise permitted by law. § 603(d).

Limitation on Creditors

Under the FACT Act amendments, credit unions will be prohibited from obtaining or using a consumer's medical information for determining credit eligibility, except as permitted under NCUA regulations for operational, transactional, and other necessary and appropriate reasons. Those NCUA regulations have not yet been issued.

However, a credit union would be permitted to disclose and use medical information in connection with the business of insurance or annuities, or as permitted under Health Insurance Portability and Accountability Act (HIPAA). § 604(g).

ADVERSE ACTION NOTICES

If a credit union takes any type of adverse action based in whole or in part on information from a consumer report, the credit union must notify the consumer.

The term "adverse action" is defined very broadly under the FCRA. It now includes *all* business, credit, and employment actions affecting consumers that can be considered to have a negative impact. These may include such actions as denying credit, denying the opening of a credit union account, offering credit on less favorable terms than requested, changing contract or credit terms, denying employment or a job promotion.

Changes have been made to the content requirements of adverse action notices under the FCRA. Credit unions should be sure that they use newly revised adverse action forms to be sure of compliance. The notices must include:

- Disclosure of the name, address, and telephone number of the CRA;
- A statement that the CRA did not make the decision to deny the requested service and is not able to explain why the decision was made;
- A statement of the consumer's right to a free disclosure of their file from the CRA if requested within 60 days; and
- A statement that the consumer has a right to dispute directly with the CRA the accuracy or completeness of the information provided in the report. § 615(a).
- The following information, if a credit score is used in taking any adverse action:
 - The numerical credit score used;
 - The range of possible scores under the model used;
 - Key factors that adversely affected the credit score;
 - The date on which the score was created; and
 - The name of the person or entity that provided the score.

The credit union must also provide the consumer with the copy of the consumer report and the Summary of Consumer's Rights *before* taking any adverse action in regard to *employment matters* (except in investigations of suspected employee misconduct). The CRA is required to supply the credit union with the Summary of Consumer Rights whenever it provides a report for employment purposes. § 604(b).

A Federal Trade Commission (FTC) Staff Opinion letter elaborates: The law is silent as to how long the employer must wait after making the pre-adverse action disclosure before actually taking adverse action; it states only that the specified items be provided before the adverse action is taken. Employers may wish to consult with their counsel in order to develop procedures that are appropriate, keeping in mind the clear purpose of the provision to allow consumers to discuss the report with employers before adverse action is taken.

If an adverse action regarding a *credit transaction* is based in whole or in part on information from a third party other than a CRA (e.g., a credit reference, employer, or family member), the credit union must also disclose that information from an outside source was used in the decision, and that the consumer may make a written request within 60 days for disclosure of the nature of the information. § 615(b).

The FCRA's adverse action requirements are separate from the adverse action notice requirements under Reg. B (which relate only to credit-related transactions). See *ii Release No. B041*. The League's form #82029 is designed to meet the current requirements of both the FCRA and Reg. B only in regard to credit-related transactions. For example, it may be used for loans and for deposit accounts that have a credit feature attached. A different form, such as The League's Deposit Account Adverse Action Notice Based on Consumer Report (#82058) may be used in connection with member deposit accounts to comply with the FCRA if there is no credit feature attached. See Exhibit A for a sample of form #82058.

An alternative form must be used to comply with FCRA adverse action notice requirements regarding employment. See *ii Release No. 0166*.

Including mortgage loan modification denial information

The League's *ii Release No. B075* explains a set of nine Reg. Z and Reg. X rules that affect how credit unions must service mortgage loans, effective Jan. 10, 2014. Among them, the release explains that Reg. X has "loss mitigation" rules that apply to most closed-end real estate transactions involving 1- to 4-family residential structures. (See Reg. X §1024.41(c) & (d) and Comment 41(d).)

Those rules says that if a consumer applies for loss mitigation – an alternative to foreclosure that the servicer might offer – and if the servicer denies the consumer for any trial or permanent loan modification option, then the servicer must notify the consumer about that denial. The notice must include certain information. Reg. X says that the credit union may combine this notice with other notices legally required notices, such as a Reg. B adverse action notice or a Fair Credit Reporting Act notice, unless otherwise prohibited by applicable law. (Reg. X Comment 41(d)(1)-3.)

IDENTITY THEFT

The FACT Act adds several provisions to the FCRA to help fight identity theft. These provisions have various effective dates.

Making Information Available to Victims

As of June 1, 2004, if a credit union does business with an identity thief, it will have to provide a copy of any application or transaction records it has to the victim or to police, upon request.

This does not mean the credit union must keep any special records. It may use records that are obtained, maintained or retained in the ordinary course of business.

Before providing any information, the credit union must verify the victim's identity. When requesting copies of documents, the victim must provide the following as proof of identity:

- A government issued ID;
- Personally identifying information of the same type that the identity thief provided to the credit union; or
- Personally identifying information that the credit union typically requests from new applicants or for new transactions (e.g., the information typically gathered under the credit union's Customer Identification Program).

The credit union can refuse to provide any information if it does not have a "high degree of confidence" in knowing the true identity of the person who is claims to be the victim, or if the request is based on a misrepresentation, or if the person could obtain the information via the Internet or other online service.

How can the credit union know whether a claim of identity theft is real? It can ask for a copy of the police report showing the victim's claim; a properly completed copy of the FTC's standardized affidavit of ID theft; or an affidavit of fact that the credit union considers acceptable for that purpose.

The request for information must be in writing and mailed to an address specified by the credit union. The credit union may ask the ID theft victim to include relevant information about any transaction alleged to result from ID theft, such as the date of the application or transaction, and the account or transaction number.

Once the credit union receives the request, along with the appropriate ID and claim, it has 30 days to provide the victim with the requested information. It cannot charge the victim for information.

Good faith disclosure under this section of the FACT Act will shield the credit union from civil liability. § 609(e).

USING "PRESCREENED LISTS"

Many lenders that solicit new credit card accounts or other loan products use prescreening to identify potential customers for the products they offer. Prescreened offers — sometimes called "preapproved" offers — are based on information in the consumer's credit report file that indicates the consumer meets criteria set by the offeror. Usually, prescreened solicitations are sent via mail, but they may also get them in a phone call or in an email. If a consumer decides that they don't want to receive prescreened offers of credit (and insurance), they have two choices — they can opt out of receiving them for five years or opt out of receiving them permanently.

The FCRA permits credit unions to obtain very limited consumer report information for use in connection with unsolicited offers of credit under certain circumstances. This practice is known as “prescreening.” It typically involves asking a consumer reporting agency to provide a list of consumers who meet certain criteria for creditworthiness. The credit union must commit to making a “firm offer of credit” to those who qualify for inclusion on the prescreened list, subject to very limited conditions set forth below.

For example, a credit union may ask its credit bureau to screen the credit union’s membership list to determine who meets the credit union’s criteria for a credit card offer.

A consumer reporting agency may only honor requests for prescreened lists in connection with any credit transaction if the consumer authorizes the agency to provide such report to such person, or:

- the transaction consists of a firm offer of credit;
- there is not in effect an election by the consumer to have the consumer’s name and address excluded from lists of names provided by the consumer reporting agency; and
- the consumer report does not contain a date of birth that shows that the consumer has not attained the age of 21, or, if the date of birth on the consumer report shows that the consumer has not attained the age of 21, such consumer consents to the consumer reporting agency to such furnishing.

Use of prescreened lists

In order to use prescreened lists the credit union must, among other things:

- before the prescreening, establish the specific criteria that will be relied upon to make the offer;
- make a “firm offer of credit” to those who qualify for inclusion on the prescreened list; and
- maintain the criteria on file for three years after the offer is made to the consumer.

Limits on information received

In a prescreened list, the credit union may receive only:

- the name and address of a consumer;
- an identifier that is not unique to the consumer and that is used by the person solely for the purpose of verifying the identity of the consumer; and
- other information pertaining to a consumer that does not identify the relationship or experience of the consumer with respect to a particular creditor or other entity.

Firm offer of credit

The term “firm offer of credit” means any offer of credit or insurance to a consumer that will be honored if the consumer is determined, based on information in a consumer report on the consumer, to meet the specific criteria used to select the consumer for the offer, except that the offer may be further conditioned on one or more of the following:

- *Application.* The consumer being determined, based on information in the consumer’s application for the credit, to meet specific criteria bearing on credit worthiness as applicable, that are established:
 - (A) before selection of the consumer for the offer; and
 - (B) for the purpose of determining whether to extend credit or insurance pursuant to the offer.
- *Verification:*
 - (A) that the consumer continues to meet the specific criteria used to select the consumer for the offer, by using information in a consumer report on the consumer, information in the consumer’s application for the credit, or other information bearing on the credit worthiness or insurability of the consumer; or
 - (B) of the information in the consumer’s application for the credit, to determine that the consumer meets the specific criteria bearing on credit worthiness or insurability.

The verification may be done through credit reports, information in the application, or other information bearing on the consumer's creditworthiness.

- *Collateral.* The consumer furnishing any collateral that is a requirement for the extension of the credit or insurance that was:
 - (A) established before selection of the consumer for the offer of credit or insurance; and
 - (B) disclosed to the consumer in the offer of credit or insurance.

Disclosure with each solicitation

With each solicitation, the credit union must provide the consumer with a clear and conspicuous statement that:

- information contained in the consumer's consumer report was used in connection with the transaction;
- the consumer received the offer of credit because the consumer satisfied the criteria for credit worthiness under which the consumer was selected for the offer;
- if applicable, the credit or insurance may not be extended if, after the consumer responds to the offer, the consumer does not meet the criteria used to select the consumer for the offer or any applicable criteria bearing on credit worthiness or does not furnish any required collateral;
- the consumer has a right to prohibit information contained in the consumer's file with any consumer reporting agency from being used in connection with any credit or insurance transaction that is not initiated by the consumer; and
- the consumer may exercise the right referred to in the previous bullet point by notifying the consumer reporting agency or the agency's established notification system (with its telephone number included).

Maintaining criteria on file

A credit union that makes an offer of credit to a consumer under a prescreened list described above must maintain all of the following on file for a 3-year period beginning on the date on which the offer is made to the consumer:

- the criteria used to select the consumer to receive the offer,
- all criteria bearing on credit worthiness or insurability, as applicable, that are the basis for determining whether or not to extend credit or insurance pursuant to the offer, and
- any requirement for the furnishing of collateral as a condition of the extension of credit or insurance.

DUTY TO FURNISH ACCURATE INFORMATION

As a general matter, a credit union may not knowingly supply inaccurate information to a CRA. If the credit union learns that information it provided to a CRA is not complete or accurate, it must promptly notify the CRA and provide the information which is complete and accurate. Thereafter, only the complete and accurate information may be reported. § 623(a).

Duties When Notified by Consumer

- If a consumer notifies the credit union that specific information is inaccurate, and the information is in fact inaccurate, the credit union must thereafter report the correct information to CRAs. Credit unions may provide consumers with an address to which the consumers may write to notify the credit union that specific information is inaccurate.
- If a consumer notifies the credit union that he or she disputes the completeness or accuracy of any information it reported, the credit union may not later report the information to a CRA without providing notice of the dispute. § 623(a).

Duties When Notified by CRA of Consumer's Dispute

If a consumer notifies a CRA that it disputes information reported by the credit union, the CRA must provide notice of the dispute to the credit union within five business days. The *CFPB Bulletin 2013-09* reinforces the requirement to promptly investigate a consumer's credit report dispute and review "all relevant information" provided by CRAs about the dispute, consisting of documents that the CRA includes with the notice of dispute or transmits during the investigation, and the credit union's own information relating to the dispute. In general, with respect to disputes received by credit unions from CRAs, the CFPB expects each credit union to comply with the FCRA by:

- (1) Maintaining a system reasonably capable of receiving from CRAs information regarding disputes, including supporting documentation;
- (2) Conducting an investigation of the disputed information including reviewing:
 - a. “all relevant information” forwarded by the CRA and;
 - b. the credit union’s own information with respect to the dispute;
- (3) Reporting the results of the investigation to the CRA that sent the dispute;
- (4) Providing corrected information to every nationwide CRA that received the information if the information is inaccurate or incomplete; and
- (5) Modifying or deleting the disputed information, or permanently blocking the reporting of the information if the information is incomplete or inaccurate, or cannot be verified.

The credit union must complete this process within 30 days of when the CRA receives notice of the dispute. (Remember, up to five business days may already have passed.) This 30-day period is extended to a total of 45 days if the consumer later provides additional relevant information to the CRA. § 623(b).

DUTY TO REPORT VOLUNTARY CLOSING OF CREDIT ACCOUNT

If the credit union regularly reports information to a CRA, the credit union must report the fact that a member has voluntarily closed a previously opened credit account any time that such is the case. The information is to be provided to the CRA when the credit union reports on the time period in which the account is closed. This rule does not apply to credit unions that rarely furnish information to CRAs. § 623(a)(4).

DUTY TO REPORT DATES OF DELINQUENCIES

If the credit union reports to a CRA that a delinquent account has been placed for collection, charged off, or subject to similar action, the credit union must also provide the date of delinquency on the account, which is the “month and year of the commencement of the delinquency on the account that immediately preceded the action.” The credit union must provide the date of the delinquency within 90 days after first reporting to the credit bureau the placement for collection or charge-off. Credit union compliance with this requirement enables the CRA to determine how long it may keep the information in the consumer’s file. § 623(a)(5).

The FTC indicates that if the creditor reports the date of the action, rather than the date of the commencement of the delinquency that immediately preceded the action, the creditor is in violation of the FCRA. The FTC provides several examples to illustrate the point:

- A consumer falls behind on monthly payments in January 1998, brings the account current in June 1998, pays on time and in full every month through October 1998, and thereafter makes no payments. The creditor charges off the account in December 1999.
- In this case, the most recent delinquency began when the consumer failed to make the payment due in November 1998. The earlier delinquency is irrelevant. The creditor must report the November 1998 date within 90 days of reporting the charge-off. For example, if the creditor charges off the account in December 1999, and reports this charge-off on December 31, 1999, the creditor must provide the month and year of the delinquency (i.e., “November 1998”) within 90 days of December 31, 1999.
- A consumer’s credit account becomes delinquent on April 15, 1998. The consumer makes partial payments for the next five months but never brings the account current. The merchant places the account for collection in May of 1999.
- Since the account was never brought current during the period that partial payments were made, the delinquency that immediately preceded the collection commenced in April 1998 when the consumer first became delinquent.

Special rules under the FACT Act allow third-party collectors to report alternate dates if they cannot obtain a date of delinquency from the credit union.

LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in federal enforcement actions, as well as private lawsuits. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Enforcement of the FCRA is administered by the FTC for state-chartered credit unions and by the NCUA for federal credit unions. §§ 616, 617 & 621.

WISCONSIN SECURITY FREEZE LAW

Under state law (Wis. Stats. §100.54) a Wisconsin consumer can place a “security freeze” on his or her consumer credit report. This can reduce the risk of identity theft and other credit fraud by preventing release of information to unauthorized persons.

For a fee of up to \$10, a CRA must give a person who asks for a security freeze a personal identification number, password, or other device to authorize release of a consumer report. The security freeze, in effect, “locks” the individual’s credit report and credit score from being released to extend credit unless the individual specifically authorizes it. The security freeze must be requesting in writing, by certified mail.

Someone with a security freeze may authorize release of a consumer credit report when he/she wants to apply for credit by contacting the CRA, providing proper identification and password, specifying the time period for which the release is authorized, and, if applicable, paying another fee of up to \$10. Wisconsin law also authorizes CRA to impose a fee for removal of a security freeze.

The CRA is not required to release the report sooner than three business days following the request. Until the report is released, a third party asking for it can treat the application for credit as incomplete.

The security freeze law does not apply to information the credit union may request with respect to a person’s existing accounts or contracts with the credit union. It also does not apply to anyone with a legitimate business need for the information in connection with a business transaction initiated by the individual. Also, the law does not apply to all CRAs. For example, it does not apply to a check services company that issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic fund transfers, or similar methods of payment.

REPORTING AFTER ERROR NOTICE ON MORTGAGE LOANS

The League’s *ii Release No. B075* explains a set of nine Reg. Z and Reg. X rules that affect how credit unions must service mortgage loans, effective Jan. 10, 2014. Among them, the release explains that Reg. X has Error notice and information request rules that apply to most closed-end real estate transactions involving 1- to 4-family residential structures. Servicers (even “small servicers”) must follow certain rules when they get error notices – written notices from the consumer that assert certain specified errors.

Reg. X requires that for 60 days after receipt of an error notice on a covered mortgage loan, the credit union may not furnish adverse information to any consumer reporting agency regarding any payment that is the subject of the error notice. (Reg. X §1024.35(i).)

* * * * *

League publications are designed to provide accurate information with regard to the subject matter covered, with the understanding that The League does not render legal services. If you have general questions regarding this release, please call The League at (608) 640-4050 if local; or (800) 242-0833. For specific legal advice, please consult your credit union’s attorney.

Legal Affairs Department

PEG/jb

© 2024 Wisconsin Credit Union League

EXHIBITS

Exhibit A – Deposit Account Adverse Action Notice Based on Consumer Report

Exhibit B – WCUL Guide to the FACT Act

EXHIBIT A – DEPOSIT ACCOUNT ADVERSE ACTION NOTICE BASED ON CONSUMER REPORT**DEPOSIT ACCOUNT ADVERSE ACTION NOTICE****Based on Consumer Report**

(For use with noncredit accounts and services.)

Date _____	Consumer's name _____
Credit Union _____	Consumer's address _____
Address _____	Date of Consumer's request (if any) _____
City, State, Zip _____	Account No. _____
Telephone _____	

Statement of Account Denial, Termination, or Change

Please read this notice carefully. It contains information about an account you recently applied for or about your existing account(s) at the Credit Union. If you have any questions regarding this notice, contact the Credit Union at the address above.

DESCRIPTION OF ACTION TAKEN BY CREDIT UNION

The credit union has taken the following adverse action(s):

- ☐ Denied your request for the following account(s) or services(s): _____
- _____
- ☐ Made the following adverse changes to your account(s) or services(s): _____
- _____
- ☐ Terminated the following account(s) or service(s): _____
- _____
- ☐ Other: _____
- _____

DISCLOSURE OF USE OF INFORMATION OBTAINED FROM AN OUTSIDE SOURCE

Our decision was based in whole or in part on information obtained in a report from the consumer reporting agency listed below. You have a right under the Fair Credit Reporting Act to know the information contained in your credit file at the consumer reporting agency. The reporting agency played no part in our decision and is unable to supply specific reasons for the action noted above. You also have a right to a free copy of your report from the consumer reporting agency noted below if you request it no later than 60 days after you receive this notice. In addition, if you find that any information contained in the report you receive is inaccurate or incomplete, you have the right to dispute the matter with the reporting agency.

Name: _____

Address: _____

Toll-free telephone number: _____ Website address: _____

- ☐ If checked, we also obtained your credit score from this consumer reporting agency and used it in making our decision. Your credit score is a number that reflects the information in your credit report. Your credit score can change, depending on how the information in your credit report changes.

Your credit score: _____ Date: _____ Scores range from: a low of _____ to a high of _____

Key factors that adversely affected your credit score: _____

_____ ☐ Number of recent inquiries on credit report.

If you have any questions regarding your credit score, you should contact the consumer reporting agency listed above.

EXHIBIT B – GUIDE TO THE FACT ACT



Guide to the FACT Act

Exhibit B to *ii Release No. 0126*

For updates, visit the Compliance Resources page at www.theleague.coop

Guide to the FACT Act - Table of Contents

EXHIBIT B – GUIDE TO THE FACT ACT	13	Prescreened Solicitations	36
INTRODUCTION	15	Indirect Lending	36
What’s New	15	Multiple Consumers	37
For Help	16	Model Forms	37
DISCLOSURES OF CREDIT SCORES BY MORTGAGE		MEDICAL INFORMATION	37
LENDERS	16	“Medical Information” Defined.....	37
Risk-Based Pricing Notice.....	17	General Prohibition	38
NOTICE OF NEGATIVE INFORMATION	17	Exception for Unsolicited Information	38
IDENTITY THEFT PROVISIONS	19	Exception for Financial Information	38
ID Theft Report	19	Specific Exceptions	39
Credit Unions’ Duties upon Notice of ID Theft	20	Sharing of Medical Information with Affiliates	42
Giving Information to ID Theft Victims	20	IMPROVING CREDIT REPORT ACCURACY	42
Notice by Debt Collectors Concerning ID Theft.....	21	Accuracy & Integrity Guidelines.....	42
CRAs to Block ID Theft Information	21	Putting Policies and Procedures in Place.....	43
Summary of Rights for ID Theft Victims	21	Content of Policies and Procedures.....	44
ID Theft Model Form, Procedures	22	Periodic Review	44
ALERTS ON CREDIT REPORTS	22	Investigations of Direct Disputes by Consumers	44
Fraud Alerts	22	Exceptions.....	45
Active Duty Alerts	23	Dispute Notices	45
DOCUMENT DISPOSAL	23	Credit Union’s Duties	46
NOTICE OF RIGHT TO “OPT-OUT” OF PRESCREENED		Address Discrepancies	46
SOLICITATIONS	24	Standard of Care	47
INFORMATION SHARING WITH AFFILIATES FOR		ID THEFT PREVENTION PROGRAM (THE “RED FLAG”	
MARKETING	25	RULES).....	47
Using vs. sharing information	25	Covered accounts.....	47
Privacy & FCRA Notices	25	Conducting a Risk Assessment.....	48
Definitions	26	1. Identify Covered Accounts.....	48
The rule and exceptions	27	2. Identify Applicable Red Flags.....	48
Contents of the notice.....	28	3. Rate Risk Levels	51
Which affiliate is to provide the notice	29	4. Plan Responses.....	51
How consumers can opt out.....	29	5. Document the Risk Assessment	52
Delivery of the notice.....	29	Board Involvement	52
Effective at least five years.....	30	Program Components	52
Renewal.....	30	ID Theft “Red Flag” Guidelines.....	53
Effective date	30	Credit/Debit Card Address Change Requests	54
RISK-BASED PRICING NOTICE	31	Examination Procedures and FAQs	55
General Requirements.....	31	TRUNCATION OF ACCOUNT NUMBERS	55
Definitions	31	FREE CREDIT REPORT	56
Methods to Determine Who Gets Notice	31	Disclosure of Credit Scores by CRAs	56
Method 1 - Consumer-to-Consumer Comparison.....	32	Truncation of Social Security Numbers.....	56
Method 2 - Credit Score Proxy Method	32	OTHER HELPFUL RESOURCES	57
Method 3 - Tiered Pricing Method	33	EXHIBIT B1 – Model Form for Initial Opt-out notice (Single-	
Alternative for Credit Card Issuers	33	Affiliate Notice).....	58
Timing & Content Risk-Based Pricing Notice	33	EXHIBIT B2 – Model Form for Initial Opt-out notice (Joint	
Account Review	34	Notice).....	59
Exceptions.....	35	EXHIBIT B3 – Model Form for Renewal Notice (Single-	
Credit Score Disclosure Exception for Mortgage Loans.....	35	Affiliate Notice).....	60
Credit Score Disclosure Exception for Non-Mortgage Credit.....	36	EXHIBIT B4 – Model Form for Renewal Notice (Joint Notice).....	61
Credit Score Disclosure Exception When No Credit Score is		EXHIBIT B5 – Model Form for Voluntary “No Marketing”	
Available.....	36	Notice	62

INTRODUCTION

Congress passed the Fair & Accurate Credit Transactions Act (or FACT Act) last year to amend the Fair Credit Reporting Act (FCRA). The FACT Act makes some sweeping changes to the FCRA, and credit unions will have to change their practices to remain in compliance.

Some of these changes went into effect in March 2004. Others are scheduled to go into effect December 1, 2004.

However, FACT Act compliance is a pretty confusing subject just now. Many parts of the FACT Act require federal regulators – including the Federal Trade Commission (FTC) and the National Credit Union Administration (NCUA) – to issue new regulations, which will tell us exactly what is required for compliance.

Some of these regulations have been finalized, but many have not even been issued in proposed form yet. Until all of the regulations are final, credit unions face a confusing array of new rules with different effective dates.

For that reason, the League presents this “WCUL Guide to the FACT Act,” to help you understand all the new FCRA provisions. We have noted which areas need your immediate attention and which are less important right now. We’ve also provided some basic information on areas that are awaiting new regulations – so that you at least have a “heads-up” on some of the issues that credit unions will face.

The information in this Guide is organized in order of its current significance to credit unions. Those new requirements that need your immediate attention are listed first. Less significant requirements or those awaiting implementing regulations are listed later.

Eventually, all of this material will be added to the main body of League’s *ii Release No. 0126* when the regulations are completed. At that time, the material will be organized differently, for example, with all of the identity theft provisions compiled together.

In the meantime, while regulations are pending, the Guide it is available as Exhibit C in that release.

As new regulations are finalized, it is hoped that regulators will allow adequate time for all financial institutions to bring their policies and practices into compliance. The League will keep Wisconsin credit unions informed as these new regulations come out.

What’s New

Here are some of the more significant FACT Act changes, all of which are summarized in this Guide:

- Requiring mortgage lenders to disclose credit scores to applicants, along with a notice explaining the score;
- Requiring that consumers be notified when negative information is reported to a credit reporting agency (CRA);
- Allowing consumers to block ID theft information from appearing on credit reports, either by notifying the CRA or by notifying the credit union directly;
- Prohibiting credit unions from “re-polluting” credit reports, i.e., re-furnishing information based on ID-theft-related information;
- Prohibiting credit unions from selling, transferring or collecting on any debt caused by ID theft;
- Requiring certain precautions before credit unions can extend credit to consumers who have placed fraud alerts or active duty alerts on their credit reports;
- Requiring new document disposal policies;
- Giving consumers enhanced rights to opt-out of prescreened credit offers or to prohibit credit unions with sharing consumer information with affiliates (like CUSOs) for marketing purposes;
- Requiring credit unions that use risk-based lending to give notices to consumers who get credit on less-favorable terms than other borrowers;
- Requiring credit unions to reinvestigate disputed information upon request directly from a consumer;
- Requiring credit unions to reconcile potentially fraudulent consumer address information; and

- Requiring credit unions to develop policies and procedures to uncover identity theft.

For Help

As always, you can contact the League's Legal Affairs Department for assistance by calling 1-(800) 242-0833 or by emailing us at compliance@theleague.coop.

Links to additional helpful resources, including the complete text of the FCRA, with FACT Act amendments, are included at the end of this Guide.

DISCLOSURES OF CREDIT SCORES BY MORTGAGE LENDERS

Immediate attention required; new regulations not needed; effective 12/01/2004

As explained later in this Guide, the FACT Act lets consumers get their credit scores and other information directly from CRAs. However, it also requires credit unions that offer mortgage loans to disclose the credit score used in connection with a mortgage loan application. The requirement applies to both closed-end loans and open-end lines of credit secured by 1-to-4 units of residential real property.

The FCRA does not specify exactly when the disclosure must be made, other than to say "as soon as reasonably practicable." The disclosure must include:

- The current or most recent consumer credit score of the consumer calculated by the CRA;
- The range of possible credit scores under the model used;
- All key factors that adversely affected the credit score;
- The date on which the credit score was created; and
- The name of the person or entity that provided the credit score or credit file on which the credit score was created.

The credit union must also give a notice to home loan applicants that explains that lenders are required to give them credit scores, what a credit score is, how it lenders use a credit score to determine credit worthiness and interest rates, and who to contact with questions concerning the score (CRA) or the loan's terms (lender). Model notice language is provided in the Act itself:

Notice to the Home Loan Applicant

In connection with your application for a home loan, the lender must disclose to you the score that a consumer reporting agency distributed to users and the lender used in connection with your home loan, and the key factors affecting your credit scores.

The credit score is a computer generated summary calculated at the time of the request and based on information that a consumer reporting agency or lender has on file. The scores are based on data about your credit history and payment patterns. Credit scores are important because they are used to assist the lender in determining whether you will obtain a loan. They may also be used to determine what interest rate you may be offered on the mortgage. Credit scores can change over time, depending on your conduct, how your credit history and payment patterns change, and how credit scoring technologies change.

Because the score is based on information in your credit history, it is very important that you review the credit-related information that is being furnished to make sure it is accurate. Credit records may vary from one company to another.

If you have questions about your credit score or the credit information that is furnished to you, contact the consumer reporting agency at the address and telephone number provided with this notice, or contact the lender, if the lender developed or generated the credit score. The consumer reporting agency plays no part in the decision to take any action on the loan application and is unable to provide you with specific reasons for the decision on a loan application.

If you have questions concerning the terms of the loan, contact the lender.

The FCRA says that lenders are not required to:

- Explain the information from the CRA that is being passed on to the mortgage applicant;
- Disclose any other information;
- Disclose any credit score or related information obtained by the lender after a loan has closed;
- Provide more than one disclosure per loan transaction; or
- Provide the disclosure required by this subsection when another person has made the disclosure to the consumer for that loan transaction.

Provisions related to the disclosure of credit scores by mortgage lenders appear in the FACT Act at §212(c), which amends FCRA §609(g), which appears in the United States Code at 15 U.S.C. §1681g (g).

Risk-Based Pricing Notice

Under different FACT Act rules, a credit union that uses risk-based pricing must give consumers a notice when, based on the consumer's credit report, it offers credit on terms that are materially less favorable than it offers to a substantial proportion of other consumers. This requirement is explained in more detail in the section titled, "Risk-Based Pricing Notice." The rules include three methods credit unions can use to determine which consumers should get the notice.

The rules also include three exceptions, allowing a credit union to give a different disclosure (which includes the consumer's credit score and information about how it relates to other consumers' scores). To take advantage of these exceptions, the credit union needs to provide credit score information to all consumers who apply for risk-based credit as soon as reasonably practicable after a credit score is obtained.

One of the exceptions applies to mortgage loans, where the disclosure of credit scores is already required. Instead of also requiring credit unions to send a risk-based pricing notice, mortgage lenders can add disclosures to supplement the mortgage loan disclosure. Credit unions that do risk-based lending can give this three-page integrated notice to all consumers who apply for closed-end loans or open-end lines of credit secured by 1-to-4 units of residential real property. To qualify for this exception, the integrated notice must disclose certain information, most importantly, the consumer's credit score and either a distribution of credit scores or a statement about how the consumer's score compares to other consumers who are scored under the same system. Regulators have provided a model form for this integrated notice, and the section titled, "Risk-Based Pricing Notices," includes a link to it.

NOTICE OF NEGATIVE INFORMATION

Immediate attention required; regulations finalized; effective 12/01/2004

The FACT Act requires that financial institutions give a "clear and conspicuous" written notice to consumers when negative information is provided to a CRA.

"Negative information" means information concerning the consumer's delinquencies, late payments, insolvencies, or any form of default.

The following Q&A answers some of the common questions regarding the Notice of Negative Information requirements.

Q: Do All Credit Unions Have to Give This Notice?

Not necessarily. The FACT Act only requires financial institutions to give the notice if they regularly extend credit and furnish information to a CRA. If you don't report to a CRA, you do not have to furnish this notice.

Q: What Should the Notice Say?

The Federal Reserve Board has issued two versions of model notice language.

As explained in more detail later, financial institutions must provide this notice *before* OR no later than 30 days *after* furnishing negative information to a CRA.

Here is the model notice language that credit unions may use if they give the notice *before* furnishing the negative information to a CRA:

We may report information about your account to credit bureaus. Late payments, missed payments, or other defaults on your account may be reflected in your credit report.

Here is the model notice language that credit unions may use if they give the notice *after* they have already furnished negative information to a CRA:

We have told a credit bureau about a late payment, missed payment or other default on your account. This information may be reflected in your credit report.

Q: Do We Have to Use Exactly That Model Language?

Using the model language ensures compliance with the FACT Act, but it is not required. Take care if you use other language.

The Federal Reserve Board has given the following examples of modest changes that may be made to the model language but still ensure compliance with the FACT Act:

- Rearranging the order of the references to "late payment(s)" or "missed payment(s)."
- Pluralizing the terms "credit bureau," "credit report," and "account."
- Specifying the particular type of account on which information may be furnished, such as "credit card account."
- Changing the first sentence in the model language that financial institutions may use prior to furnishing the negative information to state, "We may report to credit bureaus information about your account."

However, changes that are so extensive as to affect the substance, clarity, or meaningful sequence of the model language will no longer ensure FACT Act compliance.

Q: Where Can My Credit Union Buy These Notice Forms?

You don't need special forms to provide this notice. You can simply print out the two-sentence model language on credit union letterhead.

In fact, the rules say that the notice may be provided *on* or with a notice of default, billing statement, or any other information provided to the consumer, as long as it is "clear and conspicuous." For example, you can simply revise your delinquency notices to add the Notice of Negative Information language.

The FACT Act Notice of Negative Information may not be included in the initial Truth in Lending disclosures for open-end credit, though; it has to be separate. For open-end credit, Truth in Lending disclosures are typically incorporated into the credit agreement. Therefore, the Notice of Negative Information cannot be inserted into the League's Kwik Cash or R.E.A.P.® agreements or the credit union's credit card agreement. The notice can be provided at the time of the agreements, but in separate documents.

Q: When Should We Give the Notice?

A policy of waiting to provide the notice *after* submitting negative information may not be ideal. It would be easy for someone at the credit union to forget, or wait longer than 30 days, which could be a violation of federal law. (There is a "safe harbor" provision in the law, though: The FACT Act rules say that financial institutions will not be liable for failure to comply with these notice requirements if, at the time of failure, the institution maintained reasonable policies and procedures to comply with the requirements, or the institution reasonably believed it was prohibited by law from contacting the consumer.)

The better policy might be to give the notice *before* you report any negative information to a credit bureau.

But how long before? The FACT Act simply says you can provide the notice "prior to" submitting negative information. Technically, you can just give the notice at loan closing. (The notice may not be provided with the initial Truth in Lending disclosures for open-end credit, though; it has to be separate.)

However, some commentators are saying that Congress probably intended for lenders to give the notice *just* before first reporting negative information to a CRA.

For that reason, you might consider a "belt and suspenders" approach. 1) Give the notice when you close the loan. 2) In addition, incorporate the FACT Act model language into your usual delinquency notices. You'll be giving the notice at least twice that way, and you cannot be faulted for over-compliance.

Q: Who Do We Give the Notice To?

The FACT Act says to give the notice to the “customer,” which is not defined. Does that include co-signers and guarantors? Until the regulators clarify things, you should give the notice to borrowers, co-borrowers, co-signers and guarantors, at the time the loan is closed (but not in the same document in which you provide the initial Truth in Lending disclosures for open-end credit). Again, you may be over-complying, but that’s the most cautious approach.

It may be a good idea to have all of the parties sign the notice, to acknowledge receipt. The FACT Act does not require such signatures, but they could later be used to prove compliance with the FACT Act requirements.

Q: How Many Times Do We Have to Give the Notice?

Once per account. After providing the notice, the institution can later submit more negative information to the credit bureau about the same transaction, credit extension, account, or consumer without providing another notice to the member.

Q: Do We Have to Report Negative Information to a CRA?

No. Reporting to a CRA is voluntary. Also, if you provide the FACT Act “before” notice (i.e., the one that says, “We may report information about your account to credit bureaus ...”), you are not required to follow through with submitting any information to a CRA at all.

Q: Is Notice Needed When Reporting Overdrawn Deposit Balances to ChexSystems?

The jury is still out. Some commentators are telling credit unions they must provide the notice if they report overdrafts to an organization like ChexSystems. Others say no, the notice requirement only applies to extensions of credit, not overdrafts.

America's Credit Unions is seeking clarification from the regulators. Until they shed some light on this issue, however, credit unions have to decide for themselves whether to include the FACT Act notice in their collection letters or NSF notices for overdrawn accounts.

Some credit unions are adding the language just in case it later becomes clear that the notice is required. Even if it’s never required, the notice may encourage overdrawn accountholders to think about paying up.

Provisions related to the notice of negative information appear in the FACT Act at §217(a), which amends FCRA §623(a)(7), which appears in the United States Code at 15 U.S.C. 1681s-2(a)(7).

IDENTITY THEFT PROVISIONS

Significant; regulation status varies; see subsections below

The amended FCRA give consumers new tools to help remedy identity theft – which the FTC defines as a fraud that is committed or attempted using a person’s identifying information without authority. Significantly, it will allow consumers to block ID theft information from appearing on credit reports, either by notifying the CRA or by notifying the credit union directly. Once notified, credit unions will be prohibited from “re-polluting” credit reports, i.e., re-furnishing information based on ID-theft-related information. Credit unions also will be prohibited from selling, transferring or collecting on any debt caused by ID theft.

Many other parts of the FACT Act also touch on ID theft issues. For example, the FACT Act requires the regulators to jointly issue guidelines for financial institutions to use in identifying ID theft patterns and practices. Since these guidelines are not issued yet, they are of less immediate concern to credit unions and are taken up later in the Guide.

ID Theft Report

Final rules issued, effective 12/01/2004

How will credit unions and CRAs know whether a consumer has actually been the victim of identity theft? Consumers who allege identity theft can block ID theft information from their consumer reports and can stop creditors from re-furnishing such information, as explained below.

But some people may submit an ID theft report to remove accurate, but negative, information from their consumer reports. To prevent such misuse of ID theft reports for credit repair scams, the FTC’s rule requires that consumers who are ID theft victims must provide a copy of an official, valid report that the victim has filed with a federal, state or local law enforcement agency. The report must allege the ID theft with as much specificity as possible. It must include, for example, specific dates relating to the ID theft such as when the loss or theft of personal information occurred or when the fraud(s) occurred; how the consumer discovered the theft; any known information about the perpetrator; and account numbers or other relevant information related to the ID theft.

Within certain limitations, the credit union may request reasonable additional information to help them determine if ID theft actually occurred. The FTC provides some example of when it would or would not be reasonable to request additional information:

- A law enforcement report containing detailed information about the identity theft and the signature, badge number or other identification information of the individual law enforcement official taking the report should be sufficient on its face to support a victim's request. In this case, without an identifiable concern, such as an indication that the report was fraudulent, it would not be reasonable to request additional information or documents.
- If the law enforcement report is missing certain important information such as the consumer's date of birth or Social Security number, you could accept the report, but it would be reasonable to require that the consumer provide the missing information.
- A consumer might provide a law enforcement report generated by an automated system with a simple allegation that an identity theft occurred. In that case, it would be reasonable for you to ask that the consumer fill out the Federal Trade Commission's Identity Theft Report or a similar form and provide some form of identification document. In 2016 the new FTC Identity Theft Report replaced the FTC Identity Theft Affidavit that you may have seen in the past. You can easily recognize the Report — it's marked "Federal Trade Commission" at the top, features the FTC seal, and contains a unique FTC report number for each person reporting identity theft.

If you receive an Identity Theft Report from a consumer, it means:

- The consumer has reported the identity theft to the FTC under penalty of perjury. The consumer's signature on the Identity Theft Report indicates the consumer is serious about the identity theft that occurred, and about fighting back against it.
- The FTC has made the consumer's Identity Theft Report available to police and other law enforcement agencies nationwide for investigation, facilitating a coordinated law enforcement response to a crime that affects millions of people each year.
- The FTC's Identity Theft reporting site is available at: <https://www.identitytheft.gov/#/>

You have 15 days after receiving an ID theft report to ask for additional information or documents. If you receive the requested information 11 days or more later, you then have five days to decide whether to accept the report. If you receive the requested information sooner, then you must make your decision on accepting the report within 15 days from the date you first requested additional information.

The FTC regulations regarding ID theft reports appear at 12 CFR 1022.3.

Credit Unions' Duties upon Notice of ID Theft

No new regulations needed; effective 12/01/2004

If the consumer submits an identity theft report to the credit union, as described previously, the credit union cannot report any ID theft-related information to the CRA unless it later knows or is informed by the consumer that the information is correct.

Once notified of an ID theft, the credit union is prohibited from selling, transferring or placing for collection any debt caused by ID theft.

In addition, a credit union cannot furnish or refurnish consumer reports with any identity-theft related information once it is notified by a CRA. (Refurnishing such information is commonly called "re-pollution" of consumer reports.) Credit unions will be required to have "reasonable procedures" to prevent the re-pollution.

Provisions regarding CU duties upon notice of ID theft appear in the FACT Act at §154, which amends FCRA §623(a)(6), which appears in the United States Code at 15 U.S.C. §1681s-2(a)(6).

Giving Information to ID Theft Victims

No regulations needed; effective 12/01/2004

If the credit union does business with an identity thief, the FCRA requires the credit union to give a copy of the application and any business transaction records to the victim or to law enforcement upon request.

This section does not impose any additional record-keeping requirements.

Before providing any information, the credit union must verify the victim's identity – unless it has a “high degree of confidence” that it knows the individual's identity already.

The victim must give the credit union with the following at the time of the request:

- A government issued ID;
- Personally identifying information of the same type as was given to the credit union by the unauthorized person; or
- Personally identifying information that the credit union typically requests from new applicants or for new transactions, including the information described above.

As proof of the claim of ID theft, the credit union should obtain an ID theft report, as described previously.

The request must be in writing and mailed to an address specified by the credit union. In addition, the credit union may ask the ID theft victim to include relevant information about any transaction alleged to result from ID theft, such as the date of the application or transaction, and the account or transaction number.

Once the credit union gets the request, along with the appropriate ID and claim, it has 30 days to provide the victim with the requested information. The credit union may not charge the victim for providing any information.

However, the credit union can decline to provide the information if:

- It does not have a “high degree of confidence” that it knows the true identity of the person who is asking for the information; or
- The request is based on a misrepresentation; or
- The person could obtain the information via Internet or other online service.

Good faith disclosure under this section of the FACT Act will shield the credit union from civil liability.

Provisions regarding giving information to ID theft victims appear in the FACT Act at §151(e), which amends FCRA §609(e), which appears in the United States Code at 15 U.S.C. §1681g(e).

Notice by Debt Collectors Concerning ID Theft

No regulations needed; effective 12/01/2004

If the credit union uses a third party debt collector, and that collector is notified that information relating to the debt may be fraudulent or the result of ID theft, then the debt collector must notify the credit union. The FCRA also requires the collector to provide certain information to the victim.

Provisions regarding the notice by debt collectors concerning ID theft appear in the FACT Act at §155, which amends FCRA §615(g), which appears in the United States Code at 15 U.S.C. §1681m(g).

CRA's to Block ID Theft Information

No new regulations needed; effective 12/01/2004

Consumer reporting agencies must block information that the consumer claims was the result of ID theft. The consumer must give the CRA proof of identity, an identity theft report, and a statement that the information was not related to any transaction by the consumer. The CRA will be required to notify whoever furnished the information (potentially, the credit union) that it has blocked the information.

Provisions requiring CRA's to block ID theft appear in the FACT Act at §152, which amends FCRA §605B, which appears in the United States Code at 15 U.S.C. 1681c-2.

Summary of Rights for ID Theft Victims

Consumer reporting companies are required to notify consumers of their rights under the FACT Act and steps they can take to protect themselves against identity theft. The FTC, in consultation with the NCUA and other federal banking agencies, has issued model summaries for this purpose.

They have also issued model notices for consumer reporting agencies to provide to those who furnish and those who use consumer reports about their obligations under the FCRA. These notices explain to businesses their duties under the FCRA.

Credit unions do not have to distribute these summaries or notices.

Copies of the FTC's summaries and notices are available online as follows:

- Summary of Consumer Identity Theft Rights: Remediating the Effects of Identity Theft is at: <https://www.ecfr.gov/current/title-12/chapter-X/part-1022/appendix-Appendix%20I%20to%20Part%201022>
- Summary of Consumer Rights Under the Fair Credit Reporting Act is at: <https://www.ecfr.gov/current/title-12/chapter-X/part-1022/appendix-Appendix%20K%20to%20Part%201022>
- Notice to Furnishers of Information: Obligations of Furnishers Under the Fair Credit Reporting Act is at: <https://www.ecfr.gov/current/title-12/chapter-X/part-1022/appendix-Appendix%20M%20to%20Part%201022>
- Notice to Users of Consumer Reports: Obligations of Users Under the Fair Credit Reporting Act is at: <https://www.ecfr.gov/current/title-12/chapter-X/part-1022/appendix-Appendix%20N%20to%20Part%201022>

Provisions regarding the summary of rights for ID theft victims appear in the FACT Act at §151(a), which amends FCRA §609(d), which appears in the United States Code at 15 U.S.C. §1681g(d).

ID Theft Model Form, Procedures

Model form finalized; effective May 2, 2005.

Federal regulators, including the FTC and the NCUA, have developed a model Identity Theft Report form and procedures that identity theft victims can use for contacting and informing law enforcement, creditors, and consumer reporting agencies of the fraud.

This information is published on an FTC webpage for victims at www.identitytheft.gov. The FTC describes the site as a one-stop resource for people to report identity theft to law enforcement and get a personal recovery plan that responds to their specific identity theft circumstances.

The FTC's *Identity Theft Report* replaces the *FTC Identity Theft Affidavit* that you may have seen in the past. You can easily recognize the Report — it's marked "Federal Trade Commission" at the top, features the FTC seal, and contains a unique FTC report number for each person reporting identity theft.

The FTC says that if you receive an Identity Theft Report from a consumer, it means:

- *The consumer has reported the identity theft to the FTC* under penalty of perjury. The consumer's signature on the Identity Theft Report indicates the consumer is serious about the identity theft that occurred, and about fighting back against it.
- *The FTC has made the consumer's Identity Theft Report available to police* and other law enforcement agencies nationwide for investigation, facilitating a coordinated law enforcement response to a crime that affects millions of people each year.
- *Your business records may contain inaccurate information* about the consumer because of the identity theft. For example, your records may show an account the consumer did not open or authorize, or charges for goods or services the consumer did not buy. The Report and customized letters are designed to help you easily identify the accounts, charges, or other information the consumer is disputing as fraudulent.

Consumers prepare their *FTC Identity Theft Report* at <https://www.identitytheft.gov/#/>

Provisions regarding model forms for reporting ID theft appear in the FACT Act at §153, which amends FCRA §621(f)(2), which appears in the United States Code at 15 U.S.C. §1681s(f)(2).

ALERTS ON CREDIT REPORTS

Significant; some rulemaking pending, but effective 12/01/2004

Under the FCRA, consumers can place alerts on their credit reports to warn lenders that the consumer has been the victim of fraud or that the consumer is in active military service. If such an alert appears on a credit report, the FCRA requires the credit union to take certain steps (such as verifying a loan applicant's identity) before the credit union can grant credit, issue additional credit cards, or raise a credit limit.

Fraud Alerts

The FACT Act establishes a fraud alert system that notifies all prospective users of consumer reports that a consumer has been a victim of fraud or attempted fraud, including identity theft. (The consumer may also allow an alert to be placed on

a credit report if the consumer can assert in good faith that he/she are or may be about to become a victim of fraud or identity theft.)

The Act permits consumers to request that fraud alerts be placed on their credit reports for an initial period of 90 days, or for an extended period lasting seven years.

If the consumer requests that a fraud alert be placed on his or her credit report, a credit union cannot establish a new credit plan (this does not include advances on an existing open-end plan), issue additional cards on an existing credit account, or increase any credit limit in the name of a consumer unless the credit union has reasonable policies and procedures in place to form a reasonable belief that it knows the identity of the person making the request.

For initial fraud alerts, if the consumer has specified a telephone number in the alert, the credit union cannot extend any credit until it contacts the consumer using that number, or takes other reasonable steps to verify the person's identity and confirm that the application for credit is not the result of ID theft.

For extended fraud alerts, the credit union must contact the consumer in person, at the telephone number indicated in the alert, or other reasonable contact method specified by the consumer before credit is granted, additional cards are sent, etc.

Active Duty Alerts

Under the FCRA, military personnel and reservists can ask to have "active duty alerts" placed in their credit report files if they are assigned to service away from their usual duty stations.

Active duty alerts last 12 months, but military personnel who receive extended deployments can place a subsequent active duty alert in their files.

If an active duty alert appears on a credit report, a credit union will have to take certain steps before the credit union can grant credit, issue additional credit cards, or raise a credit limit. If the consumer has specified a telephone number in the alert, the credit union cannot extend any credit until it contacts the consumer using that number, or takes other reasonable steps to verify the person's identity and confirm that the application for credit is not the result of ID theft.

Provisions regarding alerts on credit report appear in the FACT Act at §112, which amends FCRA §605A, which appears in the United States Code at 15 U.S.C. §1681c-1.

DOCUMENT DISPOSAL

Significant; regulations finalized; effective dates vary

The FACT Act requires federal agencies to adopt rules for disposal of "consumer information" from consumer reports. The FTC has issued rules for state-chartered credit union. Similar rules from the NCUA apply to federal credit unions.

Under the FTC rules, your credit union must take reasonable measures to protect against unauthorized access to or use of the information that you dispose of. This does not require perfect destruction of consumer information in every situation. To determine whether your measure are "reasonable," consider the sensitivity of the information, the nature and size of the credit union's operations, the costs and benefits of different disposal methods, and relevant technological changes.

The FTC rules include the following examples of reasonable disposal measures, which are intended to serve as guidance; you may choose other appropriate measures:

- Burning, pulverizing, or shredding of papers containing consumer information so it cannot be read or reconstructed. Destruction or erasure of electronic media containing consumer information so it cannot be read or reconstructed.
- After due diligence, entering into and monitoring a written contract with a third party engaged in the business of record destruction to dispose of material specifically identified as consumer information in a manner consistent with this rule.

For details about these rules, see ii Release No. 0149, "Document Disposal."

Provisions regarding document disposal appear in the FACT Act at §216, which amends FCRA §628, which appears in the United States Code at 15 U.S.C. §1681w.

NOTICE OF RIGHT TO "OPT-OUT" OF PRESCREENED SOLICITATIONS

Limited significance; rules finalized; effective 08/01/2005

The FCRA lets credit unions obtain very limited consumer report information for use in connection with unsolicited offers of credit under certain circumstances. This practice is known as "prescreening." It typically involves asking a CRA to provide a list of consumers who meet certain criteria for creditworthiness.

The FCRA already requires that, with each solicitation, the credit union must give the consumer with a clear and conspicuous notice of the consumer's rights. For example, the notice tells the consumer that he/she may prohibit the use of information in his/her file in connection with future prescreened offers of credit. The FACT Act extends the duration of a consumer's opt-out from prescreened offers from two years to five years.

As required by the FACT Act, the FTC has created rules (in consultation with the NCUA) requiring that these opt-out notices must be "simple and easy to understand." The rules also establish a format, type size, and manner for presenting the notices.

These rules are effective August 1, 2005.

The rule requires a two-part "layered" notice – requiring each prescreened offer to contain a short statement informing consumers of their right to opt out and listing the toll-free number to call, as well as a longer statement providing additional information about prescreening.

The short portion of the notice should appear on the document designed to be seen first by the consumer, such as the cover letter.

The final rule also establishes requirements for the format, type size, and manner of the notices. The rule presents "model" notices. It may be helpful to look at the rule online -- www.ftc.gov/os/2005/01/050124factafrn.pdf -- to see examples of how the model notices are to appear on the pages of solicitations.

Short Notice. The rule requires that the "short notice" must be:

- In a type size that is larger than the type size of the principal text on the same page, but in no event smaller than 12-point type, or if provided by electronic means, then reasonable steps must be taken to ensure that the type size is larger than the type size of the principal text on the same page.
- On the front side of the first page of the principal promotional document in the solicitation, or, if provided electronically, on the same page and in close proximity to the principal marketing message
- Located on the page and in a format so that the statement is distinct from other text, such as inside a border; and
- In a type style that is distinct from the principal type style used on the same page, such as bolded, italicized, underlined, and/or in a color that contrasts with the color of the principal text on the page, if the solicitation is in more than one color.

Here is the model short notice:

You can choose to stop receiving "prescreened" offers of [credit or insurance] from this and other companies by calling toll-free [toll-free number]. See PRESCREEN & OPT-OUT NOTICE on other side [or other location] for more information about prescreened offers.

Long Notice. The rules require that the "long notice" must:

- Appear in the solicitation;
- Be in a type size that is no smaller than the type size of the principal text on the same page, and, for solicitations provided other than by electronic means, the type size must in no event be smaller than 8-point type;
- Begin with a heading in capital letters and underlined, and identifying the long notice as the "PRESCREEN & OPT-OUT NOTICE";
- Be in a type style that is distinct from the principal type style used on the same page, such as bolded, italicized, underlined, and/or in a color that contrasts with the color of the principal text on the page, if the solicitation is in more than one color; and
- Be set apart from other text on the page, such as by including a blank line above and below the statement, and by

indenting both the left and right margins from other text on the page.

Here is the model long notice:

PRESCREEN & OPT-OUT NOTICE: This “prescreened” offer of [credit or insurance] is based on information in your credit report indicating that you meet certain criteria. This offer is not guaranteed if you do not meet our criteria [including providing acceptable property as collateral]. If you do not want to receive prescreened offers of [credit or insurance] from this and other companies, call the consumer reporting agencies [or name of consumer reporting agency] toll-free, [toll-free number]; or write: [consumer reporting agency name and mailing address].

The rule also contains Spanish versions of the model notices.

Provisions regarding the notice of right to opt-out of prescreened solicitations appear in the FACT Act at §213, which amends FCRA §615(d)(1), which appears in the United States Code at 15 U.S.C. §1681m(d)(1).

INFORMATION SHARING WITH AFFILIATES FOR MARKETING

Rules finalized; effective January 1, 2008; compliance mandatory October 1, 2008.

Under the FCRA, consumers must be given a chance to "opt out" before a credit union uses information provided by an affiliate (and vice versa) to market products and services to the consumer. For credit unions, this rule will generally apply to information delivered from a CUSO to a credit union and from a credit union to the CUSO.

The NCUA and other financial regulators jointly issued rules to implement this section of the FCRA. The Federal Trade Commission is issuing substantially similar rules that apply to CUSOs.

Using vs. sharing information

The rules govern the *use* of information by an affiliate; different rules govern the *sharing* of information among affiliates.

The FCRA permits affiliates to share certain kinds of information without limitation, but *sharing* other kinds of consumer information requires an opt-out notice. A different opt-out requirement applies if an affiliate *uses* the information that was shared for marketing purposes.

- Under section 603(d)(2) of the FCRA, a credit union can share information with its affiliate (and vice versa) about the credit union’s own experiences with a member. No privacy disclosure or opt-out notice is needed (except for medical information). This kind of information is often referred to as “transaction and experience information.”
- Section 603(d)(2) limits the sharing of information that relates to the experiences *of third parties* with the member, such as credit reports or other third party verifications. This is often referred to as “other” information. It may be shared with a CUSO or other affiliate only if the member is given a clear and conspicuous disclosure that the information may be shared and the member is given the chance, before the information is shared, to opt-out (i.e., to direct that the information not be shared).
- Section 624 of the FCRA limits an affiliate’s *use* of shared information for marketing. This section applies to most any consumer information – whether it is “transaction and experience” information or “other” information. The final refers to this as “eligibility information,” which is defined below.

If an affiliate wants to use eligibility information from a credit union (or vice versa) for marketing – whether it’s “transaction and experience” information or “other” information – a disclosure and opt-out notice is needed, unless certain exceptions apply.

Thus, certain affiliate information will be subject to two opt-outs under the FCRA: a sharing opt-out and a marketing use opt-out. The regulators say, however, that this affiliate marketing opt-out notice can be combined with other required disclosures, such as the information sharing disclosure.

Privacy & FCRA Notices

The NCUA’s privacy rules do not restrict a credit union from sharing information with affiliates, but (as explained in the previous section) the FCRA rules do. The NCUA requires that your privacy disclosures must include any disclosures that you make under the FCRA regarding the ability to opt out of information sharing among affiliates. As a result, regulators have said that “The affiliate sharing notice ... of the FCRA generally must be included in the ... privacy notice, which must be provided in writing, or if the consumer agrees, electronically.”

The privacy rules do not currently have model language that reflects these FCRA disclosures. However, federal regulators are developing a model privacy form that will incorporate the affiliate marketing opt-out notice and other needed FCRA disclosures.

If combined with the privacy notices, the consumer should be allowed to exercise the opt-out in the same manner and be given the same amount of time as provided for any opt-out that is included in the privacy notice.

For more information on the NCUA privacy rules, and what your privacy notices must include, see The League's *ii Release No. 0152*.

Definitions

- *Affiliate* – This term has the same meaning as used in the FCRA's rules on sharing medical information, as discussed elsewhere in this release. It means any company that is related by common ownership or common corporate control with another company. It includes an operating subsidiary of a bank or savings association, and a credit union service organization that is controlled by a credit union. For purposes of the regulation, NCUA presumes that a federal credit union has a controlling influence over the management or policies of a credit union service organization if it is 67 percent owned by credit unions.
- *Company* – This term has the same meaning as used in the FCRA's rules on sharing medical information, as discussed elsewhere in this release. It means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.
- *Common ownership or common corporate control* – This term has the same meaning as used in the FCRA's rules on sharing medical information, as discussed elsewhere in this release. It means a relationship between two companies under which one company has, with respect to the other company:
 - Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;
 - Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or
 - The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the Board determines.

The definition also applies when any one person has a relationship like the three described above over both companies.

- *Clear and conspicuous* – reasonably understandable and designed to call attention to the nature and significance of the information.

Credit unions are encouraged, but not required, to use:

- Clear and concise sentences, paragraphs, and sections.
- Short explanatory sentences.
- Bullet points.
- Definite, concrete, everyday words.
- Active voice.
- Avoiding double negatives and legal and highly technical terms.
- Avoiding explanations that are imprecise and subject to different interpretations.

Also, "designed to call attention" may include:

- Plain language heading.
- Typeface and type size that is easy to read.
- Wide margins and ample line spacing.

- Boldface and italics for key words.

It may be necessary to use distinctive type sizes, styles, fonts, paragraphs, headings, graphics, groups, or other devices when combining affiliate marketing information with other information, like newsletters and account statements. (The credit union can combine its affiliate marketing opt-out notice with other required disclosures, like the privacy disclosures the NCUA requires.)

Notice on a web page may use text or cues to encourage scrolling down the page if necessary to view the entire notice. Try to be sure that other elements (like pop-up ads, text, graphics, hyperlinks, or sound) do not distract attention from the affiliate marketing notice.

- *Eligibility information* – Information bearing on the consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is expected to be collected or used to at least some extent as a factor in establishing credit or insurance eligibility and is used primarily for personal, family, or household purposes. Aggregate or blind data that does not contain personal identifiers is not included.
- *Pre-existing business relationship* – A relationship between an entity, or its licensed agent, and a consumer based on the following:
 - A financial contract between the entity and consumer that is in force on the date the solicitation is sent;
 - A financial transaction (including an active account or policy in force or other continuing relationship) or the purchase, rental, or lease of goods or services during the 18-month period before the date the solicitation is sent to the consumer; or
 - An inquiry or application by the consumer regarding a product or service offered by the entity that was made during the three-month period before the solicitation is sent to the consumer.

An inquiry includes a consumer’s request for information (where the consumer would reasonably expect to receive information from the affiliate about its products or services). An “inquiry” would not occur if the consumer did not provide contact information to the affiliate.

- *Solicitation* – Marketing by an entity of a product or service based on eligibility information received from an affiliate, including information in a common database that is accessible by the entity that is intended to encourage the consumer to buy or obtain a product or service. This would include telemarketing, direct mail, or email, but not communications directed to the general public, even if intended to encourage the purchase of products and services. This would also include information received by the entity’s service provider.

The rule and exceptions

In a nutshell, three conditions must be met before a credit union can use eligibility information about a consumer that it receives from an affiliate (or vice versa) for marketing solicitations:

- There must be a clear and conspicuous disclosure to the consumer in writing (or electronically if the consumer agrees) in a concise notice that eligibility information from an affiliate may be used for marketing solicitations.
- The consumer must have a reasonable opportunity to prohibit, or “opt-out,” of these solicitations.
- The consumer does not “opt-out.”

The requirement to provide the notice and opt-out does not apply when:

- The affiliate receiving the information has a pre-existing business relationship with the consumer. (This may include CUSOs that provide mortgage or other financial services.)
- The information is used to communicate with a person whom the affiliate provides services for on behalf of the individual’s employer.
- The information is used to perform services on behalf of an affiliate, although solicitations may not be sent if that affiliate is not permitted to send solicitations because the consumer elected to opt-out.
- The information is used in response to a communication about products and services initiated by the consumer. This does not include:
 - Requests for information not related to products or services;

- A consumer's response to a message left by the affiliate; or
- Solicitation of additional products and services, as part of that communication.
- The information is used to make a solicitation that the consumer authorized or requested. A pre-selected check box or boilerplate language in a disclosure will not be sufficient. The authorization terminates if it is revoked by the consumer.
- If compliance with these provisions would prevent the affiliate from complying with state insurance laws pertaining to unfair discrimination.

Contents of the notice

The affiliate marketing notice must be clear, conspicuous and concise. It must accurately disclose the following:

- The name of the affiliate providing the notice.
- A list of the affiliates, or types of affiliates, the notice covers.
- A general description of the types of eligibility information that can be used to make solicitations.
- A statement that the consumer may elect to limit the use of eligibility information to make solicitations to the consumer.
- A statement that the election will apply for a stated period of time, at least five years, and that the consumer can renew the election. (The opt-out period may be longer than five years and there is no requirement that there be an expiration date, in which case the opt-out applies until the consumer revokes it.
- If the notice is provided to consumers who have previously opted-out, such as if the notice is provided annually, a statement that there is no need to act again until a renewal notice is received.
- A reasonable and simple method for the consumer to opt-out.

The term "concise" means reasonably brief and the opt-out rights for these affiliate sharing provisions may be combined with other notices required by law, such as the GLBA privacy notices.

The notice may provide choices as to which types of information, affiliates, or methods of delivery may be subject to the opt-out, as long as one of the choices is to opt-out on *all* types of eligibility information, affiliates, and methods of delivery.

The credit union or its affiliate can choose to provide broader opt-outs than permitted under the rule.

The rule also provides model notices that may be used, but they are not required. If they are used, they provide a "safe harbor," meaning that they are deemed to comply with the requirements for clear, conspicuous, and concise notices. Certain changes may be made to model forms without losing that protection so long as they don't affect the "substance, clarity, or meaningful sequence of the language in the model forms." Acceptable changes include, for example:

1. Rearranging the order of the references to "your income," "your account history," and "your credit score."
2. Substituting other types of information for "income," "account history," or "credit score" for accuracy, such as "payment history," "credit history," "payoff status," or "claims history."
3. Substituting a clearer and more accurate description of the affiliates providing or covered by the notice for phrases such as "the [ABC] group of companies," including a statement that the entity providing the notice recently purchased the consumer's account.
4. Substituting other types of affiliates covered by the notice for "credit card," "insurance brokerage," or "securities brokerage" affiliates.
5. Omitting items that are not accurate or applicable. For example, if a person does not limit the duration of the opt-out period, the notice may omit information about the renewal notice.
6. Adding a statement informing consumers how much time they have to opt out before shared eligibility information may be used to make solicitations to them.
7. Adding a statement that the consumer may exercise the right to opt out at any time.

8. Adding the following statement, if accurate: “If you previously opted out, you do not need to do so again.”
9. Providing a place on the form for the consumer to fill in identifying information, such as his or her name and address.
10. Adding disclosures regarding the treatment of opt-outs by joint consumers to comply with federal regulations.

Attached are the following model notices:

- C-1 Model Form for Initial Opt-out Notice (Single-Affiliate Notice)
- C-2 Model Form for Initial Opt-out Notice (Joint Notice)
- C-3 Model Form for Renewal Notice (Single-Affiliate Notice)
- C-4 Model Form for Renewal Notice (Joint Notice)
- C-5 Model Form for Voluntary “No Marketing” Notice

Which affiliate is to provide the notice

Whichever entity that has a relationship with the consumer must provide the affiliate marketing notice. This can be done through a joint notice with one or more affiliates, which will provide flexibility and allow just a single notice to be used. (A joint notice must indicate the common name of the affiliates or the separate identity of the affiliates if no common name is used.)

It is not necessary for each affiliate that communicates the same eligibility information to provide an opt-out notice, as long as the notice provided by the affiliate that initially communicated the information is broad enough to cover the use of the information by each affiliate that receives and uses it to make solicitations.

How consumers can opt out

After the notice is delivered, the consumer must be given a realistic period of time to decide whether to opt-out before solicitations are sent. This period of time will depend on the circumstances. Thirty days will be considered sufficient, although shorter time periods may be adequate under certain circumstances. The time period does not have to be disclosed in the notice.

The rule gives examples of reasonable and simple methods for opting out, which are similar to those used for the NCUA’s required privacy notices. These include:

- Designating a check-off box in a prominent location on the opt-out form;
- A self-addressed envelope included with the reply form and opt-out notice;
- A toll-free telephone number, which must be adequately designed and staffed to enable consumers to opt-out in a single phone call with minimal extraneous information that is provided to consumers;
- Electronic means, if the consumer agrees, such as by email or through a website; or
- Means in which the consumer may exercise the right to opt-out under both the FCRA and privacy rules by a single method.

For electronic opt-outs, one example would be to provide the notice on the website where the consumer gets the product or service, provided the consumer acknowledges receipt of the notice. Another example would be sending the notice by email if the consumer agrees. For both electronic and in-person transactions, a reasonable opportunity to opt-out would also include giving the consumer the choice to opt-out as a necessary part of the transaction, which would require the consumer to make a choice before continuing with the transaction.

Unreasonable methods would include requiring the consumer to call or write to get the opt-out form, rather than including it in the notice. Also, consumers electing to receive the opt-out notice electronically, such as by email or through the Internet, should be able to exercise the opt-out electronically; they should not have to do it in writing or be required to visit a different website without receiving a link to that website.

Delivery of the notice

The credit union or its affiliate must deliver the opt-out notice so that the consumer can reasonably be expected to receive it. Hand delivery would be one method. For electronic delivery, if agreed to by the consumer, this could include sending an email or provide a notice on the Internet website if the consumer acknowledges receipt of the notice.

In general, you are not required to show that the member received “actual” notice. For example, sending the notice to the last known address will be sufficient, even if it does not reach the consumer.

A single opt-out notice may be sent if two or more consumers obtain a product or service, such as joint account-holders, but the notice must indicate whether an opt-out by one will be considered an opt-out by all or whether each consumer may opt-out separately. However, requiring all joint account-holders to opt-out before honoring any opt-out request will not be permitted.

Effective at least five years

If the consumer opts out, it is effective for at least five years, beginning as soon as reasonably practicable after the opt-out is received, unless the consumer revokes it, either in writing or electronically.

The opt-out period may be longer than five years and there is no requirement that there be an expiration date, in which case the opt-out applies until revoked by the consumer.

Renewal

If there is an expiration date, you must give the consumer a reasonable chance to renew the opt-out for at least another five years after the initial opt-out expires. A new opt-out notice must be sent and the consumer must have a reasonable opportunity to opt-out (unless one of the exceptions discussed earlier applies). The consumer must have this opportunity to renew after each successive opt-out period expires.

The renewals may be provided either a reasonable time period before the expiration of the opt-out period, which may include sending it with the last NCUA annual privacy notice prior to the expiration of the opt-out, or any time after expiration but before solicitations are sent to the consumer. (But, if the privacy notice has a statement that the consumer does not need to opt-out again with regard to privacy, then the notice must be clear that it is necessary to opt-out again with regard to these affiliate marketing provisions.)

In addition to information that was also required in the initial opt-out notice, the renewal notice must remind the consumer that he or she had previously opted-out and that the opt-out has or is about to expire. The renewal notice must also advise the consumer that he or she must opt-out again in order to continue limiting solicitations from affiliates.

If the consumer does not renew the opt-out, all eligible information received from an affiliate may be used, including information received during the opt-out period, but which was not used at that time to send solicitations. However, if that consumer opts-out after a period of time after the initial opt-out lapses, no eligible information may be used, including information received during the time that the opt-out was not in effect.

A consumer may opt-out at any time, even if it is not in response to an opt-out notice, and the opt-out period must still be effective for at least five years.

The opt-out will still be in effect after the consumer terminates the relationship with the entity, unless it is revoked by the consumer. If the consumer then establishes a new relationship, the entity must provide a new opt-out notice that would, at a minimum, apply to eligibility information that is obtained in connection with the new relationship.

The opt-out notice is not required if none of the affiliates receiving the eligible information uses it to send solicitations to the consumer. However, if the consumer opts- out, neither the entity nor the affiliate may send marketing solicitations to that consumer.

Effective date

These rules will be effective as of January 1, 2008, although compliance will not be mandatory until October 1, 2008. Eligibility information received from an affiliate may be used to make solicitations if it is received, or placed in a common database, before October 1, 2008. The final rule will not apply to information covered under this rule that was received prior to this effective date.

Provisions regarding use of affiliate information for marketing appear in the FACT Act at §214, which amends FCRA §624, which appears in the United States Code at 15 U.S.C. §1681s-3.

The rules for credit unions are in Part 717.20 to-.28 of the NCUA Rules and Regulations.

RISK-BASED PRICING NOTICE

Regulations finalized; effective Jan. 1, 2011

A credit union that uses risk-based pricing must give consumers a notice when, based on the consumer's credit report, it offers credit on terms that are materially less favorable than it offers to a substantial proportion of other consumers. The rules include three methods credit unions can use to determine which consumers should get the notice. The notice does not include the consumer's score, but it gives the consumer a right to get a copy of his/her consumer report.

The rules also include three exceptions, allowing a credit union to give a different disclosure (which includes the consumer's credit score and information about how it relates to other consumers' scores). To take advantage of these exceptions, the credit union needs to provide credit score information to *all* consumers who apply for risk-based credit as soon as reasonably practicable after a credit score is obtained.

The regulators have provided five model notices that credit unions can use in various situations.

The Federal Reserve Board and the Federal Trade Commission jointly issued final rules on risk-based pricing. Their two versions of the rule are substantially identical, so credit unions may comply with either.

"Risk-based pricing" means setting or adjusting the price and other terms of credit to reflect the risk that a consumer might default.

General Requirements

Credit unions that use risk-based pricing must notify consumers if:

1. They use a consumer report in connection with an application or extension of credit to a consumer; and
2. Based at least in part on that report, they give credit to that consumer on "material terms" that are "materially less favorable" than the most favorable terms available to a "substantial portion" of consumers by that credit union.

The rule only covers consumer credit that is primarily for personal, family, or household purposes. Only one notice must be given to the applicant in connection with a less favorable offer, although a notice may be required later if material terms change because of a review of an existing account. This rule also does not apply to leases.

Notice is not required if:

- The credit union provides an adverse action notice;
- The consumer applies for specific material terms and is granted those terms, unless the credit union first specified those terms after it got a consumer report; or
- The consumer withdraws an application before a credit union has provided a notice (since a creditor generally is only required to provide a notice before consummation or the first transaction under an open-end plan).

Definitions

"*Material terms*" means the annual percentage rate (APR), not including a temporary initial rate or any penalty rates, as well as fixed APR options for home equity lines of credit. For credit without an APR, "material terms" means the financial term that varies and has the most significant impact on the consumer, like an annual membership fee for a charge card or any required deposit that varies based on the consumer report.

For credit cards, the material term is the APR for purchases. For credit cards without a purchase APR, it is the APR that varies and that has the most significant impact on consumers.

"*Materially less favorable*" means the credit union imposes a cost of credit for one consumer that is "significantly greater" than the cost of credit for other consumers. However, different creditors can reach different conclusions about whether certain APRs are "materially less favorable."

"*Substantial portion*" is not defined, but regulators say it does not have to be a majority of consumers, just more than a minimal percentage.

Methods to Determine Who Gets Notice

Three methods can be used to determine whether a consumer is getting materially less favorable terms than the credit union has given to a substantial proportion of other consumers.

However, as described later, under “Exceptions,” the rules include exceptions that credit unions can use in some situations – instead of the methods described in this section – if they provide credit score information to *all* consumers who apply for risk-based credit as soon as reasonably practicable after a credit score is obtained. Some credit unions may find it simpler to rely on the exceptions, rather than trying to determine which consumers must get a notice. (The exceptions cannot be used when a risk-based pricing notice is given as part of a review of existing accounts, however.)

A credit union must use the same method to evaluate all consumers getting a specific type of credit, but it can vary the methods among different products. For example, one method can be used for mortgages and another for car loans.

Notices do not have to be given to guarantors, co-signers, sureties, or endorsers, or to those who are offered credit but decline it before the notice is given.

Method 1 - Consumer-to-Consumer Comparison

This method involves comparing the material terms offered to a consumer and the material terms offered to an adequate sample of other consumers for a specific type of credit – with similar features and designed for similar purposes – such as new car loans, used car loans, student loan, unsecured credit cards, variable rate mortgages, and so forth.

To determine if the terms one consumer gets are materially less favorable than others gets, creditors should consider how much the consumer’s cost of credit would increase as a result of having the less favorable material terms and whether that difference is likely to be important to a reasonable consumer. The regulators say that different creditors using this method may reach different conclusions about whether terms are “materially less favorable” for different types of credit. For example, a credit card issuer might conclude that a 0.25% difference in the APR is not material, but a mortgage lender may conclude that a 0.25% difference in the APR is material.

Method 2 - Credit Score Proxy Method

To use this method, 1) determine a “cutoff score,” a point where approximately 40 percent of the credit union’s consumers have higher scores and approximately 60 percent have lower scores, then 2) give risk-based pricing notices to consumers with scores below the cutoff.

The final rule allows two ways to determine the cutoff score:

- The generally required method is the “sampling approach”: Calculate the cutoff score by considering the credit scores of all or a representative sample of the consumers who have gotten credit for a certain class of products.
- Those using this approach need to recalculate their cutoff scores at least every two years.
- The sampling approach will not work for all credit unions, such as those that are just starting to use risk-based pricing. Those credit unions can initially use the “secondary source approach”: Determine the cutoff score based on information from appropriate market research or third-party sources for similar products.

A credit union that gets accounts through a merger or acquisition can use account information from the party from which it got the accounts.

A credit union using this secondary source approach must recalculate its cutoff score based on a representative sample of its own consumers within one year. If it does not lend to enough new consumers during that year to recalculate its cutoff score, it can keep using the secondary source approach until it gets enough data of its own; but it has to recalculate the cutoff using the sampling approach if it gives credit to some new consumers within two years.

Regulators understand that under the credit score proxy method, consumers may get a notice even if they qualify for the most favorable terms the credit union has to offer. In that case, regulators say that the percentages can be adjusted, based on the percentage of those in the past who got less-favorable credit terms from the credit union. If an adjustment is made using historical information, it must be used for all consumers who get a specific type of credit.

What if the credit union uses more than one credit score for a consumer? A score from one CRA may be below the cutoff, while the score from another CRA may be higher.

The final rule establishes a safe harbor for the credit union to decide what it will use as the consumer’s cutoff score:

Either use the method the credit union regularly uses (e.g., rely on the consumer’s highest score, lowest score, most recent score, etc.) or use the average of the consumer’s scores.

If no score is available, assume that that consumer is getting credit on materially less favorable terms and provide a risk-based pricing notice.

The regulation includes example of how the credit score proxy method works.

Method 3 - Tiered Pricing Method

Under this method, a credit union that sets loan terms by putting a consumer in one of several pricing tiers for a specific type of credit (based on information in a consumer report) can give a risk-based pricing notice to anyone who is not within the top tier(s). This method focuses only on the number and percentage of tiers, not on the number or percentage of consumers assigned to each tier.

This method works differently, depending on how many pricing tiers a credit union has for a certain loan product.

- If the credit union has four or fewer tiers, give the notice to everyone who is not in the top tier. For example, if the credit union uses a tiered pricing structure and sets APRs at 8%, 10%, 12% and 14%, then it should give the notice to anyone getting credit at 10%, 12% or 14%.
- If the credit union has five or more tiers, give the notice to everyone who is not in the top two tiers *and* any additional tiers that comprise between 30-40% of the total number of tiers. For example, if the credit union has nine pricing tiers, the top three tiers (that is, the three lowest-priced tiers) comprise 33% of the tiers. Therefore, the credit union would give a notice to each consumer getting credit in the bottom six price tiers.

If the credit union uses different pricing tiers for different products, a separate analysis is needed for each product.

Do not consider tiers that no consumer has or is expected to qualify for, and do not consider a rarely-used top tier that is available only to those with perfect or near-perfect credit.

Alternative for Credit Card Issuers

Another alternative method is available for credit card issuers. They can use one of the three methods described above or give a risk-based pricing notice to applicants if:

- The consumer applies for a card in connection with an application program (like a direct mail offer or “take one” application) or in response to a solicitation and more than one possible purchase APR may apply; and
- Based on that consumer’s report, the card issued to the consumer does not have the lowest purchase APR available under that application or solicitation.

This provision of the final rule is written on the assumption that when a credit card issuer offers a range of rates within a single solicitation, the consumer applies for the best available rate.

A credit card issuer does not have to give the risk-based pricing notice if:

- The consumer applies for a card for which the credit union provides a single purchase APR; or
- The consumer is offered the lowest purchase APR available on the card offer he/she applied for, even if the issuer offers lower rates under a different credit card offer to other consumers.

If a credit card does not have a purchase APR, the issuer should instead use the APR that varies based on information in a consumer report and that has the most significant impact on the consumer.

Timing & Content Risk-Based Pricing Notice

The risk-based pricing notice can be given in oral, written or electronic form.

It must be given before closed-end credit is consummated (i.e., the loan documents are signed) or before the first transaction for open-end credit. In no case should it be given before credit approval is communicated to the consumer.

If an open-end credit plan is opened either in person or by telephone, and if it is for financing a purchase of some goods or services, then the notice can be given either when the first mailing is sent (such as in a mailing of the account agreement or card) or within 30 days after the credit is approved, whichever is earlier.

The notice must:

- Explain that a consumer report includes information about a consumer's credit history and describe the type of information it includes.
- State that the terms offered, like the APR, are based on information from a consumer report.
- State that the terms offered "may" be less favorable than those offered to others with better credit histories. The rule does not require it to say the terms "are" or "will be" less favorable.
- State that the consumer is encouraged to verify the accuracy of the report and has a right to dispute any inaccuracies.
- Identify each CRA that provided a report used in the credit decision.
- State that the consumer can get a free consumer report from the CRA within 60 days (in addition to the free credit report that consumers are already entitled to under the FACT Act).
- Tell the consumer how to get the free report from the CRA. The notice should include a toll-free number, if applicable, for each CRA.
- Direct consumers to the Website of the CFPB for more information.

If a credit score is used in setting material terms of credit, the notice must also include:

- A statement that a credit score is a number that takes into account information in a CRA, that the consumer's credit score was used to set the terms of credit offered, and that a credit score can change over time to reflect changes in the consumer's credit history;
- The credit score used in making the credit decision;
- The range of possible credit scores under the model used to generate the credit score;
- All of the key factors that adversely affected the credit score (not to exceed four), except that if one of the key factors is the number of enquiries made with respect to the consumer report, the number of key factors must not exceed five;
- The date the credit score was created; and
- The name of the CRA that provided the credit score.

The regulators have provided form H-1 *"Model form for risk-based pricing notice"* for use in complying with the general risk-based pricing notice requirements if a credit score is not used in setting the material terms of credit. Form H-6, a two-page "Model form for risk-based pricing notice with credit score information" is the general notice form to be used if a credit score is used in setting the material terms of credit. (Click for [page 1](#) and [page 2](#).)

Account Review

A risk-based pricing notice also has to be given to a consumer if a credit union 1) uses a consumer report as part of a review of credit already extended to a consumer, and 2) based (even in part) on that report, the credit union increases the APR.

These notices must be given when the decision to increase the APR is communicated to the consumer. If no change-in-terms notice is sent (to the extent permitted by law), then the risk-based pricing notice has to be given within five days after the increase. Keep in mind that Wisconsin's Consumer Act requires that a change-in-terms notice be sent at least 90 days in advance for any change to open-end consumer credit that is adverse to a consumer's interests with respect to any outstanding balances, or that imposes or alters a charge the Consumer Act permits.

Notices sent after an account review must include the same basic information as notices provided to credit applicants (listed in the previous section), like a statement that a consumer report includes information about the consumer's credit history. They also give consumers the right to a free credit report.

The regulators have provided form H-2 *"Model form for account review risk-based pricing notice."* for notices given in connection with account review if a credit score is not used in increasing the annual percentage rate. Form H-7, a two-page "Model form for account review risk-based pricing notice with credit score information" is the notice to be given in connection with account review if a credit score is used in increasing the annual percentage rate. (Click for [page 1](#) and [page 2](#).)

The exceptions described in the next section do not apply when a risk-based pricing notice is given as part of the account-review process.

Exceptions

Instead of using one of the three methods described earlier to determine which applicants for risk-based credit must get a risk-based pricing notice, the rules include three exceptions. Under these exceptions, risk-based lenders can instead give credit score information (and certain other disclosures) to *all* consumers who apply for risk-based credit as soon as reasonably practicable after obtaining a credit score.

These exceptions may not be used when a risk-based pricing notice is given as part of the account-review process.

In general, these disclosures must include the consumer's credit score and certain additional information about the use of consumer reports and credit scores during the underwriting process. A consumer getting one of these credit score disclosures does not have a separate right to a free credit report.

If a credit union accesses multiple scores and uses one of them to set the terms of the credit, then that specific score should be disclosed. If it uses multiple scores to set the terms of the credit, such as by averaging them, then one of those scores must be disclosed. Credit unions can also disclose multiple credit scores.

Credit Score Disclosure Exception for Mortgage Loans

Under different FACT Act rules, credit unions must give a credit score disclosure to consumers in connection with mortgage loans. Instead of also requiring credit unions to send the standard risk-based pricing notice for those loans, credit unions can add disclosures to supplement the mortgage loan disclosure. Credit unions can give this integrated notice to *all* consumers for such loans.

To qualify for this exception, the integrated notice must disclose certain information, most importantly, the consumer's credit score and either a distribution of credit scores or a statement about how the consumer's score compares to other consumers who are scored under the same system. This can be done either by a concise narrative statement, informing the consumer that his/her credit score ranks higher than a specified percentage of consumers or by using a distribution of credit scores. A distribution can be presented in a bar graph with a minimum of six bars or by a different form of graph that is clear and readily understandable. If a bar graph is used, each bar must show the percentage of consumers with credit scores in the range of scores that the bar reflects.

The notice must also include statements that:

- A consumer report is a record of the consumer's credit history and includes information about whether the consumer pays his/her obligations on time and how much the consumer owes to creditors;
- A credit score is a number that takes into account information in a consumer report;
- A credit score can change over time to reflect changes in the consumer's credit history;
- The consumer's credit score can affect whether he/she can get credit and the cost of that credit;
- The consumer is encouraged to verify the accuracy of the report and can dispute any inaccuracies;
- The consumer can get a free credit report (with information as to how this can be done); and

The integrated notice also needs the information that is already required to be disclosed for mortgage loans under the other provisions of the FACT Act. For details on what has to be in that notice, please see the section titled "Disclosures of Credit Scores by Mortgage Lenders."

Credit unions generally need to give the consumer a credit score that was used in connection with the credit decision. If the credit union uses a credit score not created by a CRA (such as a proprietary score), it can provide either the proprietary score or a credit score and associated information from a business that regularly provides this kind of information.

A credit union that does not rely on a credit score in its underwriting can buy and give to the consumer a credit score and associated information from a business that regularly provides this kind of information.

This integrated notice must be provided at or before closing (for closed-end credit) or before the first transaction (for open-end credit). It must be in writing, in a form the consumer can keep and segregated from other disclosures.

The regulators have provided form H-3, a three-page “Model form for credit score disclosure exception for loan secured by one to four units of residential real property.” (Click for [page 1](#), [page 2](#) and [page 3](#).)

Credit Score Disclosure Exception for Non-Mortgage Credit

For loans *not* secured by one to four units of residential real estate, risk-based lenders can give all applicants their credit scores and certain other disclosures, rather than using one of the three methods described earlier to determine which applicants must get a risk-based pricing notice.

Similar to the mortgage exception described in the previous section, this notice must include certain information to help the consumer put his/her credit score in context – either a distribution of credit scores or a statement about how a consumer’s score compares to others who are scored under the same system – along with general disclosures about credit scores.

Credit unions generally need to give the consumer a credit score that was used in connection with the credit decision. If the credit union uses a credit score not created by a CRA (such as a proprietary score), it can provide either the proprietary score or a credit score and associated information from a business that regularly provides this kind of information.

A credit union that does not rely on a credit score in its underwriting can buy and give to the consumer a credit score and associated information from a business that regularly provides this kind of information.

The timing of the notice for this exception is the same as that for the mortgage loan exception described in the previous section. It must be in writing, in a form the consumer can keep.

For loans involving cooperative units, credit unions can use this exception or the credit score exception for mortgage loans, whether or not the unit is considered real property under state law.

The regulators have provided form H-4, a two-page “Model form for credit score disclosure exception for loan not secured by residential real property.” (Click for [page 1](#) and [page 2](#).)

Credit Score Disclosure Exception When No Credit Score is Available

For credit unions that regularly get credit scores and regularly disclose them to all mortgage and non-mortgage applicants as described in the previous two sections, a special notice can be given when the credit score for a particular consumer is not available from the CRA that the credit union regularly uses.

The credit union does not have to seek a credit score from another CRA. Also, if it regularly gets a particular type of credit score, which is not available for a particular consumer, the credit union does not have to get a different type of score.

The credit union needs to give the consumer a notice with the same disclosure information described in the two previous sections, along with a statement that the consumer’s score was not available from the CRA.

The notice must be given to the consumer as soon as reasonably practicable after the credit score has been requested, but in any event at or before closing (for closed-end credit) or before the first transaction (for open-end credit). It must be in writing, in a form the consumer can keep and segregated from other disclosures.

The regulators have provided form H-5, a two-page “Model form for loans where credit score is not available.” (Click for [page 1](#) and [page 2](#).)

Prescreened Solicitations

A credit union does not need to give a risk-based pricing notice if it gets a consumer report that is a prescreened list and uses that report to offer credit to a consumer, even if the material terms of that offer are different from the terms it offers to others.

Indirect Lending

The creditor responsible for giving the notice is the “original creditor” – the one the obligation is initially payable to. For example, an auto dealer should give the notice if it makes a loan and then assigns it to another creditor in an indirect lending relationship. The credit union should give the notice if it is funding the loan directly, even if application is made at the dealership.

Despite these rules, the parties can determine by contract which one will send the notice. So, if the credit union is responsible for giving the notice, it can arrange for the dealer or other party to do it, as long as the credit union has policies and procedures to verify that the other party gives the notices when required. A credit score used in the notice can be the one used by the dealer or other party, even if it is different from the one the credit union used.

Multiple Consumers

If two or more consumers are given credit, a risk-based pricing notice must be given to each of them, although a single notice may be sent if they share the same address.

However, for the three credit score exceptions (for mortgages, non-mortgages, and when no credit score is available), a *separate* notice must be provided to each consumer, regardless of whether they share an address. Each such notice must only include the credit score of the consumer the notice is sent to and not the score of the other consumer(s).

Model Forms

Credit unions can change the formats of the regulators' model notices somewhat, as long as the substance, clarity, and sequence of the notice are not changed. They can include other information, like the consumer's name, transaction identification number, date, etc., that helps identify the transaction the notice applies to. Different colors, shading, graphics and icons (such as logos and insignias) can be used.

Provisions regarding the risk-based pricing notice appear in the FACT Act at § 311(a), which amends FCRA § 615(h), which appears in the United States Code at 15 U.S.C. § 1618m(h).

The rules on risk-based pricing notices for federal credit unions are in the Federal Reserve Board's Reg. V, which is at 12 CFR §1022.70 to §1022.75. The rules are substantially similar to the Federal Trade Commission's rules for state-chartered credit unions, which appear in 16 CFR §640.1 to §640.6.

MEDICAL INFORMATION

Significant; regulations finalized; effective 4/1/2006

The FACT Act prohibits creditors from obtaining or using medical information about a consumer in connection with a credit decision. It also restricts when a CRA can furnish consumer reports that contain medical information. Finally, it restricts the sharing of medical information among affiliates.

However, the FACT Act included a requirement that federal regulators put out rules to let creditors obtain and use medical information for credit purposes in certain situations. The federal banking regulators issued those rules jointly. The rules also permit affiliates to share medical information with each other in some circumstances without being considered CRAs.

For federal credit unions, these rules are contained in Part 717 of the NCUA Rules and Regulations. For state-chartered credit unions, the rules are contained in the Federal Reserve's new Regulation FF. The rules are nearly identical.

"Medical Information" Defined

The term "medical information" is very broadly defined and includes information you get directly from a consumer, not just information from a CRA. The term means information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to:

- The past, present, or future physical, mental, or behavioral health or condition of an individual;
- The provision of health care to an individual; or
- The payment for the provision of health care to an individual.

The term does not include:

- The age or gender of a consumer;
- Demographic information about the consumer, including a consumer's residence address or email address;
- Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy; or
- Information that does not identify a specific consumer.

Reg. FF § 232.1(c)(4) and NCUA Rules and Regulations § 717.3(k).

General Prohibition

The rules provide: “A creditor may not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer’s eligibility, or continued eligibility, for credit, except as provided in” the rules. The rules then go on to list a variety of exceptions to this general prohibition. Each of the exceptions is discussed in the following subsections.

These rules only apply to the use of medical information in credit determinations; they do not affect whether creditors can obtain or use medical information for other purposes. For example, these rules do not prohibit a credit union from obtaining medical information about someone to determine their qualification or fitness for employment, insurance (other than credit insurance) or other none-credit products or services. (Nevertheless, even if medical information is initially obtained or used for employment purposes, the FACT Act rules would bar the credit union from later using that information in connection with any credit determinations.)

Other federal or state laws could limit an employer’s consideration of medical information in making employment decisions. If such issues should arise, please contact The League.

Reg. FF §§ 232.1(b) and 232.1(c)(4) and NCUA Rules and Regulations §§ 717.30(b)(1) and 717.30(b)(2)(iii).

Exception for Unsolicited Information

It is not a violation of the rules to *obtain* medical information about a consumer without specifically requesting the information. A creditor can only *use* the unsolicited information – in connection with any determination of the consumer’s eligibility, or continued eligibility, for credit – if it can rely on one of the exceptions described in the next two subsections, however.

The rules provide several examples of how unsolicited medical information might be obtained:

- In response to a general question regarding a consumer’s debts or expenses, the creditor receives information that the consumer owes a debt to a hospital;
- In a conversation with the creditor’s loan officer, the consumer informs the creditor that the consumer has a particular medical condition; or
- In connection with a consumer’s application for an extension of credit, the creditor requests a consumer report from a consumer reporting agency and receives medical information in the consumer report furnished by the agency even though the creditor did not specifically request medical information from the consumer reporting agency.

Reg. FF § 232.2 and NCUA Rules and Regulations § 717.30(c).

Exception for Financial Information

The rules provide an exception that allows creditors to obtain and use “medical information” if it is the type of information that is routinely used in determining credit eligibility, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds.

For example, the rules permit a creditor to obtain and use information about:

- The dollar amount, repayment terms, repayment history, and similar information regarding medical debts to calculate, measure, or verify the repayment ability of the consumer, the use of proceeds, or the terms for granting credit;
- The value, condition, and lien status of a medical device that may serve as collateral to secure a loan;
- The dollar amount and continued eligibility for disability income, workers’ compensation income, or other benefits related to health or a medical condition that is relied on as a source of repayment; or
- The identity of creditors to whom outstanding medical debts are owed in connection with an application for credit, including but not limited to, a transaction involving the consolidation of medical debts.

To qualify for this exception, the creditor must use the medical information in a way that is no less favorable than it would use comparable information that is not “medical information” in a credit transaction.

In addition, the creditor cannot take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account.

Examples. The rules provide several examples of using medical information consistent with the exception:

A consumer includes on an application for credit information about two \$20,000 debts. One debt is to a hospital; the other debt is to a retailer. The creditor contacts the hospital and the retailer to verify the amount and payment status of the debts. The creditor learns that both debts are more than 90 days past due. Any two debts of this size that are more than 90 days past due would disqualify the consumer under the creditor's established underwriting criteria. The creditor denies the application on the basis that the consumer has a poor repayment history on outstanding debts. The creditor has used medical information in a manner and to an extent no less favorable than it would use comparable non-medical information.

A consumer indicates on an application for a \$200,000 mortgage loan that she receives \$15,000 in long-term disability income each year from her former employer and has no other income. Annual income of \$15,000, regardless of source, would not be sufficient to support the requested amount of credit. The creditor denies the application on the basis that the projected debt-to-income ratio of the consumer does not meet the creditor's underwriting criteria. The creditor has used medical information in a manner and to an extent that is no less favorable than it would use comparable non-medical information.

A consumer includes on an application for a \$10,000 home equity loan that he has a \$50,000 debt to a medical facility that specializes in treating a potentially terminal disease. The creditor contacts the medical facility to verify the debt and obtain the repayment history and current status of the loan. The creditor learns that the debt is current. The applicant meets the income and other requirements of the creditor's underwriting guidelines. The creditor grants the application. The creditor has used medical information in accordance with the exception.

The rules also include several examples of using medical information inconsistent with the exception.

A consumer applies for \$25,000 of credit and includes on the application information about a \$50,000 debt to a hospital. The creditor contacts the hospital to verify the amount and payment status of the debt, and learns that the debt is current and that the consumer has no delinquencies in her repayment history. If the existing debt were instead owed to a retail department store, the creditor would approve the application and extend credit based on the amount and repayment history of the outstanding debt. The creditor, however, denies the application because the consumer is indebted to a hospital. The creditor has used medical information, here the identity of the medical creditor, in a manner and to an extent that is less favorable than it would use comparable non-medical information.

A consumer meets with a loan officer of a creditor to apply for a mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The credit committee follows the loan officer's recommendation and denies the application because the consumer has a potentially terminal disease. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis as part of a determination of eligibility or continued eligibility for credit.

A consumer who has an apparent medical condition, such as a consumer who uses a wheelchair or an oxygen tank, meets with a loan officer to apply for a home equity loan. The consumer meets the creditor's established requirements for the requested home equity loan and the creditor typically does not require consumers to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with such loans. However, based on the consumer's apparent medical condition, the loan officer recommends to the credit committee that credit be extended to the consumer only if the consumer obtains a debt cancellation contract, debt suspension agreement, or credit insurance product. The credit committee agrees with the loan officer's recommendation. The loan officer informs the consumer that the consumer must obtain a debt cancellation contract, debt suspension agreement, or credit insurance product to qualify for the loan. The consumer obtains one of these products from a third party and the creditor approves the loan. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis in setting conditions on the consumer's eligibility for credit.

Reg. FF § 232.3 and NCUA Rules and Regulations § 717.30(d).

Specific Exceptions

The rules include nine specific exceptions to the general prohibition described above. The rules also include examples of how several of these exceptions might apply.

1. Powers of attorney. Medical information may be used to determine whether the use of a power of attorney (POA) that is triggered by a medical event or condition is necessary and appropriate. It can also be used to determine whether the consumer has the legal capacity to contract when a person seeks to exercise a POA or act as legal representative for a consumer based on an asserted medical event or condition.

Some powers of attorney are “springing,” meaning that they become effective only if the principal later becomes incompetent or disabled, or if some other event described in the POA occurs. For more information on POAs, see The League’s *ii Release No. 0168*.

2. Legal requirements. Medical information may be used to comply with applicable requirements of local, state, or federal laws.
3. Special credit programs. Medical information may be used to determine, at the consumer’s request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is designed to meet the special needs of consumers with medical conditions. Such a plan must be established and administered under a written plan that:
 - Identifies the class of persons that the program is designed to benefit; and
 - Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

The rules include this example:

A not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans in purchasing homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer’s eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. Assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

4. Fraud. Medical information may be used to the extent necessary for fraud prevention or detection.
5. Credit for medical products or services. Medical information may be used in the case of credit for financing medical products or services, to determine and verify the medical purpose of a loan and the use of the proceeds.

The rules include several examples:

- If a consumer applies for \$10,000 of credit for the purpose of financing vision correction surgery, the creditor may verify with the surgeon that the procedure will be performed. If the surgeon reports that surgery will not be performed on the consumer, the creditor may use that medical information to deny the consumer’s application for credit, because the loan would not be used for the stated purpose.
 - If a consumer applies for \$10,000 of credit for the purpose of financing cosmetic surgery, the creditor may confirm the cost of the procedure with the surgeon. If the surgeon reports that the cost of the procedure is \$5,000, the creditor may use that medical information to offer the consumer only \$5,000 of credit.
 - A creditor has an established medical loan program for financing particular elective surgical procedures. The creditor receives a loan application from a consumer requesting \$10,000 of credit under the established loan program for an elective surgical procedure. The consumer indicates on the application that the purpose of the loan is to finance an elective surgical procedure not eligible for funding under the guidelines of the established loan program. The creditor may deny the consumer’s application because the purpose of the loan is not for a particular procedure funded by the established loan program.
6. Specific requests. Consistent with safe and sound practices, medical information may be used if the consumer or the consumer’s legal representative specifically asks that the creditor use the information to accommodate the consumer’s particular circumstances. The creditor must document the request.

The rules include several examples:

- If a consumer applies for a loan and specifically requests that the creditor consider the consumer's medical disability at the relevant time as an explanation for adverse payment history information in his credit report, the creditor may consider such medical information in evaluating the consumer's willingness and ability to repay the requested loan to accommodate the consumer's particular circumstances, consistent with safe and sound practices. The creditor may also decline to consider such medical information to accommodate the consumer, but may evaluate the consumer's application in accordance with its otherwise applicable underwriting criteria. The creditor may not deny the consumer's application or otherwise treat the consumer less favorably because the consumer specifically requested a medical accommodation, if the creditor would have extended the credit or treated the consumer more favorably under the creditor's otherwise applicable underwriting criteria.
 - If a consumer applies for a loan by telephone and explains that his income has been and will continue to be interrupted on account of a medical condition and that he expects to repay the loan liquidating assets, the creditor may, but is not required to, evaluate the application using the sale of assets as the primary source of repayment, consistent with safe and sound practices, provided that the creditor documents the consumer's request by recording the oral conversation or making a notation of the request in the consumer's file.
 - If a consumer applies for a loan and the application form provides a space where the consumer may provide any other information or special circumstances, whether medical or non-medical, that the consumer would like the creditor to consider in evaluating the consumer's application, the creditor may use medical information provided by the consumer in that space on that application to accommodate the consumer's application for credit, consistent with safe and sound practices, or may disregard that information.
 - If a consumer specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit and provides the creditor with medical information for that purpose, and the creditor determines that it needs additional information regarding the consumer's circumstances, the creditor may request, obtain, and use additional medical information about the consumer as necessary to verify the information provided by the consumer or to determine whether to make an accommodation for the consumer. The consumer may decline to provide additional information, withdraw the request for an accommodation, and have the application considered under the creditor's otherwise applicable underwriting criteria.
 - If a consumer completes and signs a credit application that is not for medical purpose credit and the application contains boilerplate language that routinely requests medical information from the consumer or that indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, the consumer has not specifically requested that the creditor obtain and use medical information to accommodate the consumer's particular circumstances.
7. Forbearance agreements. Consistent with safe and sound practices, medical information may be used to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer.

The rules provide this example:

After an appropriate safety and soundness review, a creditor institutes a program that allows consumers who are or will be hospitalized to defer payments as needed for up to three months, without penalty, if the credit account has been open for more than one year and has not previously been in default, and the consumer provides confirming documentation at an appropriate time. A consumer is hospitalized and does not pay her bill for a particular month. This consumer has had a credit account with the creditor for more than one year and has not previously been in default. The creditor attempts to contact the consumer and speaks with the consumer's adult child, who is not the consumer's legal representative. The adult child informs the creditor that the consumer is hospitalized and is unable to pay the bill at that time. The creditor defers payments for up to three months, without penalty, for the hospitalized consumer and sends the consumer a letter confirming this practice and the date on which the next payment will be due.

8. Debt cancellation or suspension. Medical information may be used to determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement – if a medical condition or event is a triggering event under the contract or agreement.
9. Credit insurance. Medical information may be used to determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product – if a medical condition or event is a triggering event under the product.

Reg. FF § 232.4 and NCUA Rules and Regulations § 717.30(e).

Sharing of Medical Information with Affiliates

The FACT Act restricts the sharing of medically related information with affiliates.

If a credit union were to share information with an affiliate, and that information met the definition of a “consumer report,” the credit union could be considered a CRA. For that reason, the FCRA provides exclusions from the term “consumer report” that allow the sharing of information with affiliates – such as sharing transaction or experience information among affiliates or sharing other information among affiliates after notice and an opportunity to opt-out.

However, the FACT Act provides that these exclusions do not apply if “medically related information” is disclosed to an affiliate.

The term “medically related information” includes “medical information” (as described above) as well as an individualized list or description based on payment transactions for medical products or services, and an aggregate list of identified consumers based on payment transactions for medical products or services.

The FACT Act does, however, provide several exceptions that allow institutions to share medically related information with affiliates.

Significantly for credit unions, these exceptions allow the sharing of medically related information with affiliates for “any purpose described in section 502(e) of the Gramm-Leach-Bliley Act.” (The Gramm-Leach-Bliley Act governs the privacy of financial institution records.) That would include sharing medically related information “as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer,” or “to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction ...”

The affiliate sharing rules and exceptions are complex. For more information about them, contact The League.

Redisclosure. The FACT Act provides that any person that receives medical information as an affiliate or from a CRA must not disclose that information to anyone else, except as necessary to carry out the purpose for which the information was disclosed, or as otherwise permitted by statute, regulation, or order.

The FACT Act's statutory restrictions on sharing medical information with affiliates apply to all financial institutions. The NCUA's rules for federal credit unions contain provisions that essentially mirror the FACT Act statutes. (NCUA Rules and Regulations §§ 717.31 & .32.) No parallel rules are included in the Federal Reserve's Reg. FF, however.

Provisions regarding medical information appear in the FACT Act at §§ 411 & 412, which amend FCRA §§ 604(g) & 605(a), which appear in the United States Code at 15 U.S.C. §§ 1681b(g) & 1681c(a).

IMPROVING CREDIT REPORT ACCURACY

The Act amended the FCRA in several ways to help improve the accuracy of consumer credit reports. New NCUA guidelines will help you improve the accuracy of information you report to CRAs. The FACT Act imposes a higher duty of care on furnishers of information. Also, consumers may dispute information with credit unions directly, rather than going through a CRA. Finally, NCUA regulations require credit unions to have policies and procedures in place to deal with discrepancies in consumers' addresses.

Accuracy & Integrity Guidelines

Significant; regulations finalized; effective July 1, 2010

NCUA accuracy and integrity rules apply to FCUs; essentially identical FTC rules apply to state-chartered credit unions. The rules are effective as of July 1, 2010.

Under these rules, credit unions must have written policies and procedures (appropriate for the nature, size, complexity and scope of their activities) to ensure the accuracy and integrity of information they report to CRAs. The rule includes guidelines, which credit unions must incorporate as appropriate when developing their policies and procedures.

The policies and procedures should be designed to meet four objectives:

1. Furnishing accurate information about accounts or other relationships with consumers. “Accuracy” means that the information must:

- Identify the appropriate consumer;
 - Reflect the terms and liability for the accounts or relationships; and
 - Reflect the consumer's performance and other conduct.
2. Furnishing information with "integrity" about accounts or relationships with consumers. "Integrity" means that the information must:
- Be substantiated by the credit union's records;
 - Be furnished in a way meant to minimize the chances of it appearing incorrectly on a credit report, meaning that it should:
 - Include appropriate identifying information about the consumer; and
 - Be furnished in a standardized and understandable way, with a date to show the time period it relates to; and
 - Include the credit limit, if applicable.
- (Note: The rules define "integrity" very broadly. It can apply to almost any information in the credit union's possession about an account or relationship that would be needed to evaluate a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living. If the absence of the information would likely be materially misleading, then the information affects integrity. The rules also define "integrity" to include any factor listed in the regulators' guidelines, but the guidelines only list one factor – the credit limit, if applicable.)
3. Conducting reasonable investigations of consumer disputes and taking appropriate actions based on the outcomes. (See "Investigations of Direct Disputes by Consumers," below.)
4. Updating information furnished to CRAs, as needed, to show the current status of an account or relationship. This would include, for example:
- A transfer of an account to a third party; and
 - A cure of the consumer's breach of the account terms.

Putting Policies and Procedures in Place

When developing these policies and procedures, regulators say the credit union should consider:

- Its business activities;
- The nature and frequency of the information it furnishes to CRAs; and
- The technology it uses to furnish information.

The credit union should start by identifying practices or activities that can compromise the accuracy or integrity of information and then consider whether new practices might better protect the information. This includes:

- Reviewing existing practices and activities;
- Reviewing the credit union's records and other information about the accuracy, integrity or disputes of information provided to CRAs, and the types of errors, omissions or other problems that may have affected the accuracy and integrity of the information;
- Considering any feedback from CRAs, consumers or other parties;
- Getting feedback from credit union staff; and
- Considering the possible impact of its policies and procedures on consumers.

Next, evaluate how effective existing policies and procedures are, and update them as needed.

Finally, evaluate the credit union's methods for reporting information to CRAs – how effective they are, how they affect the accuracy and integrity of information, and whether changes might improve accuracy and integrity.

Content of Policies and Procedures

The guidelines list 13 items that the credit union's policies and procedures should address:

1. A system for furnishing information to CRAs that is appropriate to the nature, size, complexity and scope of the credit union's operations.
2. Standard data reporting formats and standard procedures for compiling and furnishing data, where feasible, such as electronic transmissions.
3. The credit union maintaining records for a reasonable time (at least as long as any applicable recordkeeping requirement) to substantiate the accuracy of any information that the consumer disputes. (See "Investigations of Direct Disputes by Consumers," below.)
4. Appropriate internal controls on the accuracy and integrity of information reported to CRAs, such as by implementing standard procedures, verifying random samples and conducting regular reviews of the information.
5. Staff training to implement these policies and procedures.
6. Appropriate and effective oversight of service providers whose activities may affect the accuracy and integrity of the information to ensure compliance with the policies and procedures.
7. Reporting to CRAs after mergers, acquisitions or transfers of accounts, in a way that prevents re-aging of the information, duplicative reporting or other problems that may affect accuracy and integrity.
8. Deleting, updating and correcting information in the credit union's records, as appropriate, to avoid furnishing inaccurate information.
9. Reasonable investigations of disputes.
10. Designing technological or other means of communicating with CRAs to prevent duplicative reporting, reporting on the wrong consumer, and other occurrences that may compromise accuracy and integrity.
11. Giving CRAs sufficient information to properly identify the consumer.
12. Periodic evaluation of the credit union's practices, CRA practices that the credit union is aware of, investigations of disputes, corrections of inaccurate information, means of communication and other factors that may affect accuracy and integrity.
13. Complying with the applicable provisions of the FCRA and its rules.

Periodic Review

The credit union must review its policies and procedures periodically and update them as needed so they continue to be effective.

Provisions regarding accuracy and integrity guidelines appear in the FACT Act at § 312(a), which amends FCRA § 623(e)(1), which appears in the United States Code at 15 U.S.C. § 1681s-2(e)(1).

The rules on accuracy and integrity for federal credit unions are in Part 717.42 of the NCUA Rules and Regulations. They are substantially similar to the Federal Trade Commission's rules for state-chartered credit unions, which appear in 16 CFR §660.3.

Investigations of Direct Disputes by Consumers

Significant; regulations finalized; effective July 1, 2010

In the past, credit unions that reported to CRAs only had to respond to consumer disputes that had been submitted to CRAs, which passed the disputes onto the credit union, typically through an automated electronic dispute system. The FCRA now says that in some circumstances, a credit union that furnishes information to a CRA must investigate a dispute over the accuracy of that information, based on a direct request by the consumer.

The credit union must conduct a reasonable investigation if the dispute relates to:

- The consumer's liability for a credit account or other debt with the credit union, such as direct disputes as to whether there has been identity theft or fraud against the consumer, whether there is individual or joint liability on an account, or whether the consumer is an authorized user of the credit account.

- The terms of a credit account or other debt with the credit union, such as direct disputes about the type of account, principal balance, scheduled payment on an account, or the amount of the reported credit limit on an open-end account, like a credit card.
- The consumer's conduct concerning the account, such as direct disputes over current payment status, high balance, date a payment was made, the amount of a payment made, or the date the account was opened or closed.
- Any other information in a credit report about an account or relationship with the credit union that bears on creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, if that information is attributed to the credit union.

Exceptions

The credit union does not need to investigate a direct dispute if it reasonably believes that the direct dispute is being submitted or prepared by a credit repair organization or if the dispute is over any of the following:

- The consumer's identifying information (other than related to the consumer's liability for an account or debt with the credit union), such as names, date of birth, Social Security number, telephone numbers and addresses;
- Identities of past or present employers;
- Inquiries or requests for a credit report;
- Information derived from public records, such as judgments, bankruptcies, liens or other legal matters (unless provided by the credit union);
- Information about fraud alerts or active duty alerts; or
- Information provided to a credit bureau by another furnisher.

The credit union does not have to investigate a direct dispute if it reasonably determines that the dispute is frivolous or irrelevant, such as when (for example):

- The consumer did not provide enough information to investigate the disputed information (although the credit union should make a good faith effort to get this information); or
- The dispute is substantially the same as a dispute previously submitted by or on behalf of the consumer, either to the credit union directly or to a CRA, and the credit union already investigated it.

If the credit union decides the dispute is frivolous or irrelevant, it must notify the consumer within five business days. The notice must be delivered by mail or other means (if authorized by the consumer). It must include the reasons for the determination and identify the information that is needed to investigate the dispute.

Dispute Notices

The dispute can be submitted to any business address of the credit union, unless the credit union designates an address for getting direct dispute. This could be either:

- An address provided by the credit union and set forth on the consumer's credit report; or
- An address the credit union clearly and conspicuously specifies for submitting direct disputes, either in writing or electronically (if the consumer agrees to electronic delivery).

The dispute notice must include the following:

Enough information to identify the account in dispute, such as an account number, and the name, address, and telephone number of the consumer, if applicable;

Specific information that the consumer is disputing and an explanation of the basis for the dispute; and

All supporting documentation or other information the credit union reasonably requires to substantiate the basis for the dispute. This may include a copy of the relevant portion of the credit report that includes the disputed information, a police report, a fraud or identity theft affidavit, a court order or account statements.

Credit Union's Duties

Once the credit union gets a dispute notice, it must conduct a reasonable investigation, review all relevant information the consumer provided, and complete the investigation generally within 30 days (with a 15-day extension available in limited circumstances). If the investigation shows the information reported was inaccurate, the credit union must promptly notify each CRA to which it provided the information and correct it.

Provisions regarding investigation of disputed information appear in the FACT Act at § 312(c), which amends FCRA § 623(a)(8), which appears in the United States Code at 15 U.S.C. § 1681s-2(a)(8).

The rules on regarding investigation of disputed information for federal credit unions are in Part 717.43 of the NCUA Rules and Regulations. They are substantially similar to the Federal Trade Commission's rules for state-chartered credit unions, which appear in 16 CFR §660.4.

Address Discrepancies

Regulations finalized; effective Jan. 1, 2008; compliance mandatory Nov. 1, 2008

Address discrepancies are important clues that a member's identity might have been stolen.

The FCRA requires consumer reporting agencies to provide a notice of address discrepancy if the address on file is "substantially" different from the one a user (like a credit union) provides when it requests a credit report about a consumer.

Credit unions that use credit reports (and that may include your human resources department) must develop reasonable policies and procedures to respond to notices of address discrepancy. Those procedures must allow the credit union to form a reasonable belief that the report it has obtained actually relates to consumer about whom it requested the information.

An address discrepancy notice is also a red flag and, therefore, the program that is developed under the red flag rules (described below) may apply here.

Here are examples of reasonable policies and procedures that a credit union could use:

- Comparing the information in the credit report with the information that the credit union:
 - Obtains and uses to verify the consumer's identity under its Customer Identification Program (CIP);
 - Maintains in its own records (such as applications, change of address notifications, other consumer account records or retained CIP documents); or
 - Obtains from third-party sources.
- Verifying the information in the credit report.

In addition, the credit union must have policies and procedures for giving a CRA a consumer's address that the credit union has reasonably confirmed is accurate, when the following three conditions are present:

- The credit union forms a reasonable belief that a consumer report relates to the consumer about whom it requested the report;
- The credit union "establishes" a continuing relationship with the consumer; and
- The credit union regularly and in the ordinary course of business furnishes information to the CRA.

The user may reasonably confirm that an address is accurate by any of the following methods:

- Verifying the address with the consumer.
- Reviewing its own records to verify the address of the consumer.
- Verifying the address through third party sources.
- Using other reasonable means.

These policies and procedures must provide that the credit union will furnish the consumer's address (which the credit union has reasonably confirmed is accurate) to the credit bureau as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

A similar requirement for existing accounts exists in Section 623 of the FCRA, which requires a credit union to promptly provide to CRAs complete and accurate information about those accounts.

Provisions regarding reconciling addresses appear in the FACT Act at § 315, which amends FCRA § 605(h), which appears in the United States Code at 15 U.S.C. § 1681c(h).

The rules on reconciling addresses for federal credit unions are in Part 717.82 of the NCUA Rules and Regulations. They are substantially similar to the Federal Trade Commission's rules for state-chartered credit unions, which appear in 16 CFR §681.1.

Standard of Care

Somewhat significant; no regulations needed; effective 12/01/2004

Under the FACT Act amendment, you may not furnish any information relating to a consumer if you know or have reasonable cause to believe that the information is inaccurate. This means "having specific knowledge, other than solely allegations by the consumer, that would cause a reasonable person to have substantial doubts about the accuracy of the information."

This is a higher standard of care than the FCRA imposed before the FACT Act revisions. Previously, the standard of care was "knows or consciously avoids knowing that the information is inaccurate."

Provisions regarding the heightened standard of care appear in the FACT Act at § 312(b), which amends FCRA § 623(a)(1), which appears in the United States Code at 15 U.S.C. § 1681s-2(a)(1).

ID THEFT PREVENTION PROGRAM (THE "RED FLAG" RULES)

Regulations finalized; effective Jan. 1, 2008. Compliance mandatory Nov. 1, 2008, for federal credit unions. Enforcement delayed for state-chartered credit unions.

All financial institutions (and other creditors) that hold any consumer accounts or other accounts with a reasonably foreseeable risk of identity theft (e.g., small business accounts) must have a written Identity Theft Prevention Program, under rules issued jointly by federal regulators. The program must be designed to detect, prevent and mitigate identity theft.

The regulators provided guidelines to help maintain an effective ID theft prevention program.

The NCUA's rules and guidelines apply to federal credit unions; the FTC's apply to state-chartered credit unions and credit union service organizations that are creditors. They are substantially similar.

Covered accounts

The ID theft program rules are risk-based, and coverage is based on the type of account involved more than whether the member is an individual consumer or a business. The rules apply to any financial institution that offer a "covered account," which includes:

- An account that is primarily for personal, family, or household purposes and permits multiple payments or transactions. This would include credit cards, checking accounts, savings accounts, individual retirement accounts, mortgage loans, car loans, consumer leases, margin accounts, cell phone accounts, and utility accounts. A share certificate would be a "covered account" under this part of the definition if the member is allowed to make multiple deposits or withdrawals.
- Any other account in which there is a reasonably foreseeable risk to consumers or to the safety and soundness of the financial institution or creditor from identity theft. This includes financial, operational, compliance, reputation, or litigation risks.

Covered accounts under this part of the definition could include accounts held by small businesses or sole proprietors (which are particularly vulnerable to identity theft), share certificates and small business loans.

The credit union will need to, on a risk basis, determine which types of accounts fall into the "other account" group for which there is foreseeable risk of ID theft. This will include a risk assessment that considers:

- The methods it provides to open its accounts.
- The methods it provides to access its accounts.
- Previous experiences with identity theft.

Conducting a Risk Assessment

A credit union's Identity Theft Prevention Program must be risk-based. This means that credit unions, like other financial institutions and creditors, need to conduct a risk assessment to determine what "covered accounts" they offer and what level of risk they face for identity theft. The risk assessment must be updated periodically, as well.

In conducting the risk assessment, the credit union should take into consideration:

- The types of covered accounts the credit union offers or maintains;
- The methods for opening covered accounts;
- The methods the credit union provides to access covered accounts;
- Previous experiences with identity theft; and
- Examples of red flags from regulators.

The credit union should involve staff from all areas of its operations to conduct the risk assessment. The results should be reduced to writing and presented to the board of directors, which is responsible for creating a risk-based Identity Theft Prevention program.

The risk assessment process can be broken down into the following five steps.

1. Identify Covered Accounts

The credit union should begin by making a comprehensive list of the "covered accounts" it offers. Then identify the methods that can be used to open or access those accounts that might be susceptible to identity theft.

All credit unions offer accounts that fall into the first category of covered accounts: accounts primarily for personal, family, or household purposes that involve or are designed to permit multiple payments or transactions (such as credit card accounts, mortgage loans, automobile loans, share draft or share accounts). The credit union may or may not offer accounts in the second category: any other accounts for which there is reasonable foreseeable risk to members or to the credit union's safety and soundness from identity theft. This category might include, for example, business accounts.

Analyze whether each type of account presents potential risks (financial, operational, compliance, reputation, or litigation) for identity theft. Take into consideration the risks to the member as well as the risks to the credit union's own operations and its safety and soundness. If there is a potential risk in any category, include it as a covered account.

For example, the credit union should consider whether a reasonably foreseeable risk of identity theft may exist in connection with business accounts that may be opened or accessed remotely, through methods that do not require face-to-face contact, such as through the Internet or telephone.

In addition, if accounts have been the target of identity theft, factor those experiences into the determination.

2. Identify Applicable Red Flags

The next step is to identify the potential red flags (patterns or practices that may indicate identity theft) that could affect your covered accounts. Check forgery or use of a stolen credit card are obvious signs of identity theft.

Each credit union needs to develop its own lists of red flags that are appropriate to the credit union's operations.

The red flags that the credit union identifies should be listed in the credit union's Identity Theft Prevention Program.

The list should be based on:

- Incidents of identity theft the credit union has experienced,
- Methods of ID theft that reflect changes in ID theft risks, and
- Guidance from regulators.

Federal regulators have provided examples of red flags, which are reprinted below. This is not an exhaustive list, and each credit union must work to add any other applicable red flags that may affect its operations or members.

In the list below, questions or comments from The League are inserted to help you to think about whether that particular red flag really is relevant to the credit union. Do not include in the credit union's Identity Theft Prevention Program any red flags that are not appropriate for the credit union's operations or resources. The credit union should not just "cut and paste" the regulator's list of examples into its policy.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member, 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.

[Does the credit union obtain consumer reports for covered accounts? If so, does the staff check the report for the issues listed above?]

Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or member presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or member presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file, such as an account agreement card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the credit union. 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.

[Does the credit union make it a policy to check the Death Master File? Does it have resources to find out whether an SSN has been issued?]

- Personal identifying information provided by the member is not consistent with other personal identifying information provided by the member. For example, there is a lack of correlation between the SSN range and date of birth.

[Some vendors may provide information on the year a SSN became available and in what state. Does the credit union have a vendor that can do this?]

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the federal credit union. For example: The address or telephone number on an application is the same as the address or telephone number provided on a fraudulent application.

[Can the credit union's system "flag" an address or telephone number from a fraudulent application, to alert staff if the same address or number is provided again in the future?]

- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the credit union. For example:
 - a. The address on an application is fictitious, a mail drop, or prison; or
 - b. The phone number is invalid, or is associated with a pager or answering service.

[Can/does the credit union check these things?]

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

[Does the credit union have a system to cross-check SSNs?]

- The address or telephone number provided is the same as or similar to those submitted by an unusually large number of other persons opening accounts or other members.

[Does the credit union have a system to identify addresses or telephone numbers provided by other applicants or members?]

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

[Does the credit union follow up on incomplete applications to see if missing information is supplied?]

- Personal identifying information provided is not consistent with personal identifying information that is on file with the credit union.
- The person opening the covered account or the member cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

[Does staff ask "challenge questions," to elicit information the real member should know?]

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

- 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.

[Does the credit union have procedures in place to alert staff of a recent change in address on a covered account?]

- A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
 - a. The member fails to make the first payment or makes an initial payment but no subsequent payments; or
 - b. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry);

[Can the credit union's system identify such transactions and flag them for staff?]

- 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; or

- d. A material change in electronic fund transfer patterns in connection with a deposit account.

[Does the credit union have resources to monitor “patterns of activity” on accounts?]

- 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).

[Does your system alert you to transactions on inactive accounts?]

- Mail sent to the member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member’s covered account.

[Is an account flagged if mail is returned as undeliverable?]

- The credit union is notified that the member is not receiving paper account statements.
- The credit union is notified of unauthorized charges or transactions in connection with a member’s covered account.

Notice From Members or Others Regarding Possible ID Theft

- The credit union is notified by a member, 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.

Other Red Flags

The following were included in the proposed red flag rules, but not in the final version of the rule. Still, the credit union may want to consider the other possible red flags as it identifies the red flags that apply to the credit union’s operations.

- The name of an employee of the financial institution or creditor has been added as an authorized user on an account.

[Can your system monitor and detect when any employee’s name has been added to an account?]

- An employee has accessed or downloaded an unusually large number of customer account records.

[Can your system detect in a practical manner whether employees have accessed or downloaded an unusually large number of customer account records?]

- The credit union detects attempts to access a customer’s account by unauthorized persons.
- The credit union detects or is informed of unauthorized access to a customer’s personal information.
- There are unusually frequent and large check orders in connection with a customer’s account.

[Would a check vendor notify the credit union of an unusual request? Would this necessarily indicate possible identity theft?]

- The person opening the account or the customer is unable to lift a credit freeze placed on his or her consumer report.

[Commenters to the proposed rule objected to this red flag being included in the list. How would the credit union know that the applicant is unable to lift a credit freeze? What if the member simply chose not to? What action would/could the credit union take in this situation?]

3. Rate Risk Levels

Determine which red flags from step 2 are most relevant for each covered account type you listed in step 1, and rate the risk that each account could encounter that type of red flag. Responsibility for spotting that red flag should be assigned to the business area that is most likely to encounter it.

4. Plan Responses

Consider how the credit union can respond to red flags that are spotted for each account type, based on the potential threat level. Regulators have suggested the following as possible appropriate responses:

- Monitoring a covered account for evidence of identity theft;
- Contacting the member;
- Changing any passwords, security codes, or other security device that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covering account to a debt collector;
- Notifying law enforcement;
- Filing a Suspicious Activity Report; or
- Determining that no response is warranted under the particular circumstances.

5. Document the Risk Assessment

Regulators have not provided a model risk assessment matrix, so each credit union will need to determine how it will conduct and document its assessment. One suggestion would be to create a template or Excel spreadsheet, in which the credit union would list the types of covered accounts, the red flags it has identified, the risk for each account type related to each red flag, and possible strategies for responding and mitigating the risks. The completed report should be presented to the board of directors,

Board Involvement

The board of directors or an appropriate committee of the board must approve the program and be involved in its oversight, development and implementation.

Oversight by the board or its committee should include:

- Assigning specific responsibility for the program's implementation.
- Reviewing annual reports prepared by staff regarding compliance with the red flags rules. The staff responsible for the development, implementation, and administration of the program should provide these reports on at least an annual basis. The report should address matters related to the program and issues, such as the effectiveness of the policies and procedures that address the risk of identity theft in connection with the opening of covered accounts or existing covered accounts, service provider arrangements, significant incidents of identity theft and management's response to these incidents, and recommendations for material changes to the program.
- Approving material changes to the program, as necessary, to address changing identity theft risks.

Program Components

The credit union's program must be appropriate to its size and complexity and the nature and scope of its activities. It must include reasonable policies and procedures that will:

- Identify relevant red flags for the covered accounts and incorporate those red flags into the program. Red flags are patterns, practices, or activities that indicate the possible risk of identity theft.
- Detect red flags when they occur.
- Respond appropriately to any red flags detected to prevent and mitigate identity theft.
- Update the program periodically to reflect changes in risks from identity theft to consumers and to the safety and soundness of the credit union.

The program can incorporate existing policies, procedures and other arrangements that may address ID theft risks. Credit unions should evaluate their existing policies and procedures and use them to help comply with these requirements to detect red flags. These may have been developed as a result of compliance with the CIP rules, the Federal Financial Institution's Examination Council's guidance on authentication, any applicable information security standards, and the

Bank Secrecy Act rules. These current policies and procedures may need to be supplemented in order to comply with these new requirements.

The credit union must also train staff, as necessary, to implement the program and exercise effective oversight of service provider arrangements.

Each credit union must also consider the “Red Flag” Guidelines, as described below, and include in its program those guidelines that are appropriate.

ID Theft “Red Flag” Guidelines

The regulators’ guidelines are titled “*Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.*” They are intended to help credit unions (and others) formulate and maintain the program. They include a supplement with a list of examples of red flags.

Identifying relevant red flags. The credit union should consider these factors in identifying relevant red flags, as appropriate:

- The types of covered accounts it offers.
- The methods for opening covered accounts.
- The methods it provides to access its covered accounts.
- Previous experiences with identity theft.
- The Guidelines’ examples of red flags.
- Credit unions should incorporate relevant red flags from the following sources:
- Incidents of identity theft that it has experienced.
- Methods of identity theft that it has identified that reflect changes in identity theft risks.
- Guidance from regulators.

The program should include relevant red flags from the following categories, as appropriate:

- Alerts, notifications, or other warnings received from credit bureaus or service providers, such as fraud detection services.
- The presentation of suspicious documents.
- The presentation of suspicious personal identifying information, such as a suspicious address change.
- Unusual use or suspicious activity related to a covered account.
- Notice from consumers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Detecting red flags. The credit union’s program should address how it will detect red flags, such as by:

- For new accounts - obtaining identifying information about, and verifying the identity of, a person opening a covered account, such as by following Customer Identification Program rules. (For details on Customer Identification, see The League’s *ii Release No. 0159.*)
- For existing covered accounts - authenticating consumers, monitoring transactions, and verifying address change requests.

Preventing and mitigating identity theft. The program’s policies and procedures should provide appropriate responses to the red flags by the credit union, commensurate with the risk that is posed. This response should consider aggravating factors that may heighten the risk of identity theft, such as a data security breach resulting in unauthorized access to an account, or notification that a consumer has provided account information to someone fraudulently claiming to represent the institution or has provided the information on a fraudulent website.

These appropriate responses may include:

- Monitoring a covered account for evidence of identity theft.
- Contacting the consumer.
- Changing passwords, security codes, or other devices that permit access to the covered account.
- Reopening the account with a new account number.
- Not opening a new covered account.
- Closing an existing covered account.
- Notifying law enforcement.
- If the incident involves an elderly member or at-risk adult, notifying an appropriate enforcement agency, [relatives, or certain other parties \(including contacts that a member may authorize in advance\)](#). For details, see The League's *ii Release No. 0174, "Reporting Financial Abuse."*
- Determining that no response is warranted under the circumstances.

Updating the program. Credit unions should update the program (and the red flags that are relevant) periodically to reflect changes in risks to the consumer or to the credit union's safety and soundness. This should be based on the following responses:

- The credit union's experiences with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that the credit union offers.
- Changes in the credit union's business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Third party service providers. If a service provider is used in connection with covered accounts, the financial institution or creditor should ensure that the activity of the service provider is conducted pursuant to reasonable policies and procedures that are designed to detect, prevent, and mitigate the risk of identity theft. These policies and procedures may differ from the ones used by the financial institution or creditor, as long as they comply with these rules.

For example, a service provider that provides an online banking platform permitting account opening or access, performs call center services that permit account access, or collects debts on delinquent accounts, would be providing services related to covered accounts to the credit union. In such cases, the credit union should take steps to ensure that the activities of such service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft in accordance with the Red Flags Rules.

Indirect Lending. For indirect lending, the dealer that initially extends credit to the consumer is responsible for applying its Identity Theft Prevention Program to the opening of that covered account. Once the loan is then assigned to the credit union, it becomes responsible for its program to the loan as an existing covered account.

Credit/Debit Card Address Change Requests

The red flag rules also require credit and debit card issuers to have policies and procedures to verify address change requests.

If the issuer gets a change-of-address request and then, within a short period of time (at least 30 days) receives a request for an additional or replacement card, it cannot issue a new card unless it takes steps to assess whether the change of address is valid. Those steps could include:

- Sending a notice to the cardholder at the cardholder's former address, alerting him/her of the request and providing the cardholder with a means to promptly report an incorrect address;
- Notifying the cardholder of the address change request by another means of communication previously agreed to by the issuer and the cardholder; or

- Using other means of evaluating the validity of the address change, in accordance with the issuer's policies and procedures that are outlined in its program, as described in the red flag rules described above.

Getting a change of address notice from the U.S. Postal Service is not enough to validate the request. A card issuer that receives a notice of a change of address from the postal system regarding a cardholder's address, and, within at least 30 days, a request for an additional or replacement card, may not issue the card unless it has validated the cardholder's address using one of the procedures in the bullet-point list above.

Whether written or electronic, a notice of an address change request must be "clear and conspicuous" (meaning "reasonably understandable and designed to call attention to the nature and significance of the information"). It must be provided separately from the regular correspondence that is sent to the consumer. Oral notices may also be provided, if outlined in the policies and procedures that the issuer has established pursuant to the red flag rules.

Your policies and procedures can provide for the verification of *all* address change requests. If you've already verified such a request before receiving a request for an added or replacement card, you need not verify the address a second time before issuing the card. The assessment does not have to be done if you've already decided that the address change request is fraudulent.

Also, based on the issuer's own experiences with identity theft, it may be smart to validate the address change request before issuing the additional or replacement card, even if the request for the card is made more than 30 days after the address change request.

The rules apply to credit and debit card issuers, which includes payroll cards, but not gift cards or other prepaid cards.

Provisions regarding the red flag guidelines appear in the FACT Act at § 114, which amends FCRA § 615(e), which appears in the United States Code at 15 U.S.C. § 1681m(e).

The rules on ID theft red flags for federal credit unions are in They are substantially similar to the Federal Trade Commission's rules for state-chartered credit unions, which appear in 16 CFR §681.2.

The rules for card issuers regarding changes of address(for federal credit unions) are in Part 717.91 of the NCUA Rules and Regulations. They are substantially similar to the Federal Trade Commission's rules for state-chartered credit unions, which appear in 16 CFR §681.3

The Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation appear in Appendix J to Part 717 of the NCUA Rules and Regulations (for federal credit unions). They also appear in Appendix A to 16 CFR Part 681(the FTC's rules for state-chartered credit unions).

Examination Procedures and FAQs

Federal regulators, including the NCUA, have jointly approved the procedures that examiners will use to determine a financial institution's compliance with the FACT Act's rules on red flags, address discrepancies and changes of address.

- The procedures for the address discrepancies rules are online at: www.federalreserve.gov/boarddocs/srletters/2008/SR0807a1.pdf
- The procedures for the red flags rules are online at: www.federalreserve.gov/boarddocs/srletters/2008/SR0807a2.pdf
- The procedures for the change of address rules are online at: www.federalreserve.gov/boarddocs/srletters/2008/SR0807a3.pdf

Federal regulators have issued a set of frequently asked questions (FAQs) about the "red flags" regulations on identity theft and discrepancies in change-of-address requests. The FAQs provide guidance on many parts of the rules. They are online at: www.ncua.gov/news/press_releases/2009/6-11RedFlagsFAQs.pdf

TRUNCATION OF ACCOUNT NUMBERS

Not significant; no regulations needed; effective as described below

Anyone that accepts credit/debit cards cannot print more than the last 5 digits of the card number or expiration date on any receipt at the point of sale or transaction. This limitation applies only to receipts that are printed electronically.

This rule may not directly affect credit unions, but will require compliance by any business that accepts credit cards or debit cards at point of sale, retail point-of-sale equipment vendors, and payment systems providers.

The rule is effective Jan. 1, 2005 for new registers/machines first put into use on or after that date. It is effective Dec. 4, 2006, for existing registers/machines that were already in use prior to Jan. 1, 2005.

Provisions regarding truncation of account number appear in the FACT Act at § 113, which amends FCRA § 605(g), which appears in the United States Code at 15 U.S.C. § 1681c(g).

FREE CREDIT REPORT

Not significant; regulations finalized; effective in phases

While of little significance to credit unions, this provision may prompt many inquiries from your members.

Consumer reporting agencies must give consumers one free credit report annually, upon request (or in connection with requests for fraud alerts). The FCRA does not require credit unions to provide these reports; instead, consumers should request them directly from the CRA.

Note: This is different from the Wisconsin law's requirement that, upon request from a customer, loan applicant or credit applicant, the credit union must provide that person, at no additional charge with a copy of any written credit report for which a fee is imposed and which relates to that individual. Wis. Stats. § 186.53.

The FTC has issued regulations to streamline the process of requesting the free annual reports. Under the FTC rules, CRAs must establish a "centralized source" for accepting consumer requests for free credit reports (called annual file disclosures in the rules). This centralized source must include a dedicated Internet site, a toll-free telephone number, and a postal address.

The FTC rules provide for a gradual roll-out of the centralized source. The centralized source will become available in cumulative stages, over a period of nine months, rolling-out from west to east beginning December 1, 2004. The entire transition will be complete by September 1, 2005. Wisconsin consumers will become eligible to get their free credit reports on March 1, 2005.

Provisions regarding free credit reports appear in the FACT Act at § 211, which amends FCRA § 612(a)(1), which appears in the United States Code at 15 U.S.C. § 1681j(a)(1).

Disclosure of Credit Scores by CRAs

Not significant

In addition to getting a free annual copy of a credit report, consumers may request their credit scores, which CRAs must provide along with a notice explaining what the score is and what it means.

Note: The FCRA does not require credit unions to provide these reports; instead, consumers should request them directly from the CRA. However, mortgage lenders should note that they must disclose credit scores to mortgage loan applicants. That requirement is explained in more detail previously.

The notice that CRAs must provide will include:

- The consumer's current credit score, or the most recent one calculated by the CRA;
- The range of possible scores under the model used;
- All of the key factors that adversely affected the consumer's credit score in the model used, not to exceed four key factors ("key factors" are all of the relevant elements or reasons adversely affecting the credit score for the particular individual, listed in order of importance based on their effect on the credit score);
- The date the score was created; and
- The name of the person or entity that provided the score or credit file upon which the score was created.

CRAs may charge a "fair and reasonable" fee for providing the score.

Provisions regarding disclosure of credit scores and key factors by CRAs appear in the FACT Act at § 212, which amends FCRA §§ 609(a) & 605(d), which appear in the United States Code at 15 U.S.C. §§ 1681g(a) & 1681c(d).

Truncation of Social Security Numbers

Not significant; no implementing regulations needed; effective 12/01/04

CRAAs must honor a consumer's request to truncate the first 5 digits of the social security number or other identification number when providing the consumer with a copy of the consumer's credit report. This requirement only applies to credit reports given to consumers, not those provided to lenders or other users, so it will have negligible impact on credit unions.

Provisions regarding the truncation of Social Security Numbers on consumers' credit reports appear in the FACT Act at § 115, which amends FCRA § 609(a)(1), which appears in the United States Code at 15 U.S.C. § 1681g(a)(1).

OTHER HELPFUL RESOURCES

The full text of the FCRA, including all of the recent FACT Act amendments, is available on the FTC's website: www.ftc.gov/os/statutes/031224fcra.pdf

America's Credit Unions posts the latest developments regarding the FACT Act here: <https://www.cuna.org/Compliance/eGuide/Fair-Credit-Reporting-Act/#NEW!>

Additional FACT Act resources (Including The League's *ii Release No. 0126 - The Fair Credit Reporting Act*) are posted on The League's Compliance Resources page. Visit www.theleague.coop, and click on "CU Resources," then "Compliance." A password is required.

Note: This document is available as Exhibit B of The League's *ii Release No. 0126 – Fair Credit Reporting Act*.

© 2016 Wisconsin Credit Union League

EXHIBIT B1 – MODEL FORM FOR INITIAL OPT-OUT NOTICE (SINGLE-AFFILIATE NOTICE)

[Your Choice to Limit Marketing]/[Marketing Opt-out]

- [Name of Affiliate] is providing this notice.
- [Optional: Federal law gives you the right to limit some but not all marketing from our affiliates. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from our affiliates.] • You may limit our affiliates in the [ABC] group of companies, such as our [credit card, insurance brokerage, and securities brokerage] affiliates, from marketing their products or services to you based on your personal information that we collect and share with them. This information includes your [income], your [account history with us], and your [credit score].
- Your choice to limit marketing offers from our affiliates will apply [until you tell us to change your choice]/[for x years from when you tell us your choice]/[for at least 5 years from when you tell us your choice]. [Include if the opt-out period expires.] Once that period expires, you will receive a renewal notice that will allow you to continue to limit marketing offers from our affiliates for [another x years]/[at least another 5 years].
- [Include, if applicable, in a subsequent notice, including an annual notice, for consumers who may have previously opted out.] If you have already made a choice to limit marketing offers from our affiliates, you do not need to act again until you receive the renewal notice.

To limit marketing offers, contact us [include all that apply]:

- **By telephone:** 1 (877) ###-####
- **On the Web:** www.---.com
- **By mail:** check the box and complete the form below, and send the form to:

[Company name]

[Company address]

☐ Do not allow your affiliates to use my personal information to market to me.

EXHIBIT B2 – MODEL FORM FOR INITIAL OPT-OUT NOTICE (JOINT NOTICE)

[Your Choice to Limit Marketing]/[Marketing Opt-out]

- The [ABC group of companies] is providing this notice.
- [Optional: Federal law gives you the right to limit some but not all marketing from the [ABC] companies. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from the [ABC] companies.]
- You may limit the [ABC] companies, such as the [ABC credit card, insurance brokerage, and securities brokerage] affiliates, from marketing their products or services to you based on your personal information that they receive from other [ABC] companies. This information includes your [income], your [account history], and your [credit score].
- Your choice to limit marketing offers from the [ABC] companies will apply [until you tell us to change your choice]/[for x years from when you tell us your choice]/[for at least 5 years from when you tell us your choice]. [Include if the opt-out period expires.] Once that period expires, you will receive a renewal notice that will allow you to continue to limit marketing offers from the [ABC] companies for [another x years]/[at least another 5 years].
- [Include, if applicable, in a subsequent notice, including an annual notice, for consumers who may have previously opted out.] If you have already made a choice to limit marketing offers from the [ABC] companies, you do not need to act again until you receive the renewal notice.

To limit marketing offers, contact us [include all that apply]:

- By telephone: 1 (877) ###-####
- On the Web: www.---.com
- **By mail:** check the box and complete the form below, and send the form to:

[Company name]

[Company address]

☐ Do not allow any company [in the ABC group of companies] to use my personal information to market to me.

EXHIBIT B3 – MODEL FORM FOR RENEWAL NOTICE (SINGLE-AFFILIATE NOTICE)

[Renewing Your Choice to Limit Marketing]/[Renewing Your Marketing Opt-out]

- [Name of Affiliate] is providing this notice.
- [Optional: Federal law gives you the right to limit some but not all marketing from our affiliates. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from our affiliates.]
- You previously chose to limit our affiliates in the [ABC] group of companies, such as our [credit card, insurance brokerage, and securities brokerage] affiliates, from marketing their products or services to you based on your personal information that we share with them. This information includes your [income], your [account history with us], and your [credit score].
- • Your choice has expired or is about to expire.

To renew your choice to limit marketing for [x] more years, contact us [include all that apply]:

- **By telephone:** 1 (877) ###-####
- **On the Web:** www.---.com
- **By mail:** check the box and complete the form below, and send the form to:

[Company name]

[Company address]

___ Renew my choice to limit marketing for [x] more years.

EXHIBIT B4 – MODEL FORM FOR RENEWAL NOTICE (JOINT NOTICE)

[Renewing Your Choice to Limit Marketing]/[Renewing Your Marketing Opt-out]

- The [ABC group of companies] is providing this notice.
- [Optional: Federal law gives you the right to limit some but not all marketing from the [ABC] companies. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from the [ABC] companies.]
- You previously chose to limit the [ABC] companies, such as the [ABC credit card, insurance brokerage, and securities brokerage] affiliates, from marketing their products or services to you based on your personal information that they receive from other ABC companies. This information includes your [income], your [account history], and your [credit score].
- Your choice has expired or is about to expire.

To renew your choice to limit marketing for [x] more years, contact us [include all that apply]:

- **By telephone:** 1 (877) ###-####
- **On the Web:** www.---.com
- **By mail:** check the box and complete the form below, and send the form to:

[Company name]

[Company address]

___ Renew my choice to limit marketing for [x] more years.

EXHIBIT B5 – MODEL FORM FOR VOLUNTARY “NO MARKETING” NOTICE

Your Choice to Stop Marketing

- [Name of Affiliate] is providing this notice.
- [Your choice to stop marketing from us and our affiliates will apply until you tell us to change your choice.] OR [insert language describing the duration of a consumer’s opt-out period.]
- You may choose to stop all marketing from us and our affiliates.

To stop all marketing, contact us [include all that apply]:

- **By telephone:** 1 (877) ###-####
- **On the Web:** www.---.com
- **By mail:** check the box and complete the form below, and send the form to:

[Company name]

[Company address]

☐ Do not market to me.