recordkeeping requirement, in order to substantiate the accuracy of any information about consumers it furnishes that is subject to a direct dispute.

(d) Establishing and implementing appropriate internal controls regarding the accuracy and integrity of information about consumers furnished to consumer reporting agencies, such as by implementing standard procedures and verifying random samples of information provided to consumer reporting agencies.

(e) Training staff that participates in activities related to the furnishing of information about consumers to consumer reporting agencies to implement the policies and procedures.

(f) Providing for appropriate and effective oversight of relevant service providers whose activities may affect the accuracy or integrity of information about consumers furnished to consumer reporting agencies to ensure compliance with the policies and procedures.

(g) Furnishing information about consumers to consumer reporting agencies following mergers, portfolio acquisitions or sales, or other acquisitions or transfers of accounts or other obligations in a manner that prevents re-aging of information, duplicative reporting, or other problems that may similarly affect the accuracy or integrity of the information furnished.

(h) Deleting, updating, and correcting information in the furnisher's records, as appropriate, to avoid furnishing inaccurate information.

(i) Conducting reasonable investigations of disputes.

(j) Designing technological and other means of communication with consumer reporting agencies to prevent duplicative reporting of accounts, erroneous association of information with the wrong consumer(s), and other occurrences that may compromise the accuracy or integrity of information provided to consumer reporting agencies.

(k) Providing consumer reporting agencies with sufficient identifying information in the furnisher's possession about each consumer about whom information is furnished to enable the consumer reporting agency properly to identify the consumer.

(l) Conducting a periodic evaluation of its own practices, consumer reporting agency practices of which the furnisher is aware, investigations of disputed information, corrections of inaccurate information, means of communication, and other factors that may affect the accuracy or integrity of information furnished to consumer reporting agencies.

(m) Complying with applicable requirements under the Fair Credit Reporting Act and its implementing regulations.

[74 FR 31524, July 1, 2009]

APPENDICES F–I TO PART 717 [RESERVED]

APPENDIX J TO PART 717—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

Section 717.90 of this part requires each federal credit union that offers or maintains one or more covered accounts, as defined in §717.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist federal credit unions in the formulation and maintenance of a Program that satisfies the requirements of §717.90 of this part.

I. The Program

In designing its Program, a federal credit union may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to members or to the safety and soundness of the federal credit union from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A federal credit union should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Federal credit unions should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the federal credit union has experienced;

(2) Methods of identity theft that the federal credit union has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

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

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from members, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the federal credit union.

III. Detecting Red Flags

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

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account; for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 1020.220); and

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

IV. Preventing and Mitigating Identity Theft

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

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

(b) Contacting the member;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Federal credit unions should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to members or to the safety and soundness of the federal credit union from identity theft, based on factors such as:

(a) The experiences of the federal credit union with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the federal credit union offers or maintains; and

(e) Changes in the business arrangements of the federal credit union, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

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

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the federal credit union with §717.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the federal credit union responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the federal credit union with §717.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the federal credit union in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a federal credit union engages a service provider to perform an activity in connection with one or more covered accounts the federal credit union should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the

risk of identity theft. For example, a federal credit union could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the federal credit union, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Federal credit unions should be mindful of other related legal requirements that may be applicable, such as:

(a) Filing a Suspicious Activity Report under 31 U.S.C. 5318(g) and 12 CFR 748.1(c);

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the federal credit union detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in appendix J of this part, each federal credit union may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings From a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in §717.82(b) of this part.

4. 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.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or member presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or member presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the federal credit union, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the federal 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.

11. 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.

12. 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:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the federal 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.

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

15. The address or telephone number provided is the same as or similar to the address

or telephone number submitted by an unusually large number of other persons opening accounts or by other members.

16. 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.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the federal credit union.

18. For federal credit unions that use challenge questions, 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.

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

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

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

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The member fails to make the first payment or makes an initial payment but no subsequent payments.

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

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

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

e. A material change in telephone call patterns in connection with a cellular phone account.

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

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

24. The federal credit union is notified that the member is not receiving paper account statements.

25. The federal credit union is notified of unauthorized charges or transactions in connection with a member's covered account.

Notice From Members, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Federal Credit Union

26. The federal 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.

[72 FR 63769, Nov. 9, 2007, as amended at 74 FR 22644, May 14, 2009; 76 FR 18365, Apr. 4, 2011]

PART 721—INCIDENTAL POWERS

Sec.

AUTHORITY: 12 U.S.C. 1757(17), 1766 and 1789.

SOURCE: 66 FR 40857, Aug. 6, 2001, unless otherwise noted.

§ 721.1 What does this part cover?

This part authorizes a federal credit union (you) to engage in activities incidental to your business as set out in this part. This part also describes how interested parties may request a legal opinion on whether an activity is within a federal credit union's incidental powers or apply to add new activities or categories to the regulation. An activity approved in a legal opinion to an interested party or as a result of an application by an interested party to add new activities or categories is recognized as an incidental powers activity for all federal credit unions. This part does not apply to the activities of corporate credit unions.