	A	B	D
3	**Identity Theft Red Flags Procedures**		
4	**INTRODUCTION AND PURPOSE**		
5	**DEFINITIONS**		
6	**EXCEPTIONS**		
7	**PENALTIES**		
8	**RECORD RETENTION REQUIREMENTS**		
9	**717.90 Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft**	**Yes/No**	**Comments**
10	1. Verify that the credit union periodically identifies covered accounts it offers or maintains. Verify that the credit union: • included accounts for personal, family, and household purposes that permit multiple payments or transactions; and • conducted a risk assessment to identify any other accounts that pose a reasonably foreseeable risk of identity theft, taking into consideration the methods used to open and access accounts, and the institution's previous experiences with identity theft. (717.90(c))		
11	2. Review examination findings in other areas (e.g. Bank Secrecy Act, Customer Identification Program and Customer Information Security Program) to determine whether there are deficiencies that adversely affect the credit union's ability to comply with the Identity Theft Red Flags Rules (Red Flag Rules).		
12	3. Review any reports, such as audit reports and annual reports prepared by staff for the board of directors (or an appropriate committee thereof or a designated senior management employee) on compliance with the Red Flag Rules, including reports that address: • the effectiveness of the credit union's Identity Theft Prevention Program (Program); • significant incidents of identity theft and management's response; • oversight of service providers that perform activities related to covered accounts; and • recommendations for material changes to the Program. Determine whether management adequately addressed any deficiencies. (717.90(f), Guidelines, Section VI(b))		

	A	B	D
3	**Identity Theft Red Flags Procedures**		
13	4. (a)Verify that the credit union has developed and implemented a comprehensive written Program, designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account. The Program must be appropriate to the size and complexity of the credit union and the nature and scope of its activities. (717.90(d)(1)).		
14	(b)Verify that the credit union considered the Guidelines in Appendix J to the regulation (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation) in the formulation of its Program and included those that are appropriate. (717.90(f))		
15	(c)Determine whether the Program has reasonable policies, procedures and controls to effectively identify and detect relevant Red Flags and to respond appropriately to prevent and mitigate identity theft. (717.90(d)(2)(i)-(iii))		
16	(d)Determine whether the credit union uses technology to detect Red Flags. If it does, discuss with management the methods by which the credit union confirms the technology is working effectively.		
17	(e)Determine whether the Program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in the risks to customers and the safety and soundness of the credit union from identity theft. (717.90(d)(2)(iv))		
18	(f)Verify that (i) the board of directors (or appropriate committee thereof) initially approved the Program; and (ii) the board (or an appropriate committee thereof, or a designated senior management employee) is involved in the oversight, development, implementation and administration of the Program. (717.90(e)(1) and (2))		
19	5. Verify that the credit union trains appropriate staff to effectively implement and administer the Program. (717.90(e)(3))		
20	6. Determine whether the credit union exercises appropriate and effective oversight of service providers that perform activities related to covered accounts. (717.90(e)(4))		

	A	B	D
3	**Identity Theft Red Flags Procedures**		
21	**717.91 Duties of Card Issuers Regarding Changes of Address**	**Yes/No**	**Comments**
22	1. Verify that the card issuer has policies and procedures to assess the validity of a change of address if: • it receives notification of a change of address for a member's debit or credit card account; and • within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. (717.91(c))		
23	2. Determine whether the policies and procedures prevent the card issuer from issuing additional or replacement cards until it: • notifies the cardholder at the cardholder's former address or by any other means previously agreed to and provides the cardholder a reasonable means to promptly report an incorrect address (717.91(c)(1)(i)-(ii)); or • uses other reasonable means of evaluating the validity of the address change; (717.91(c)(2)) In the alternative, a card issuer may validate a change of address request when it is received, using the above methods, prior to receiving any request for an additional or replacement card. (717.91(d))		
24	3. Determine whether any written or electronic notice sent to cardholders for purposes of validating a change of address request is clear and conspicuous and is provided separately from any regular correspondence with the cardholder. (717.91(e))		
25	4. If procedural weaknesses or other risks requiring further information are noted, obtain a sample of notifications from cardholders of changes of address and requests for additional or replacement cards to determine whether the card issuer complied with the regulatory requirement to evaluate the validity of the notice of address change before issuing additional or replacement cards.		

Cell: A4

Comment: In December 2003, the FACT Act (FACTA) became law. FACTA added several new provisions to the Fair Credit Reporting Act of 1970 (FCRA), one of which (Section 114) directed the FFIEC Agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft. For federal credit unions, NCUA incorporated the FACTA changes into NCUA Rules and Regulations, Part 717, Subpart J (Identity Theft Red Flags), Appendix J (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation), and Subpart I (Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal). NCUA created two sections to implement Subpart J, §717.90 (Duties regarding the detection, prevention, and mitigation of identity theft) and §717.91 (Duties of card issuers regarding changes of address). For state chartered credit unions, the Federal Trade Commission has enforcement power and added Part 681 (Identity Theft Rules) to title 16 of the Code of Federal Regulations (16 CFR 681). The Identity Theft Rules is commonly referred to as the Red Flags Rule.

Cell: A5

Comment: For purposes of section 717.70 and Appendix J, the following definitions apply:

(1) Account means a continuing relationship established by a person with a credit union to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A share or deposit account.

(2) The term board of directors refers to a credit union's board of directors.

(3) Covered account means:

(i) An account that a credit union offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, checking account, or share account; and

(ii) Any other account that the credit union offers or maintains for which there is a reasonably foreseeable risk to members or to the safety and soundness of the credit union from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) Credit has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) Creditor has the same meaning as in 15 U.S.C. 1681a(r)(5).

(6) Customer means a member that has a covered account with a credit union.

(7) Financial institution has the same meaning as in 15 U.S.C. 1681a(t).

(8) Identity theft has the same meaning as in 16 CFR 603.2(a).

(9) Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) Service provider means a person that provides a service directly to the credit union.

Cell: A6

Comment: There are no exceptions.

Cell: A7

Comment: There are no civil liability provisions in the regulation; however, state law may provide a basis for an individual to sue the credit union for compliance problems.

Cell: A8

Comment: There are no record retention requirements mentioned in the Red Flags Rule. However, a credit union would need to produce evidence to support their actions demonstrating compliance with the rule.

Cell: A10

Comment: The risk assessment and identification of covered accounts is not required to be done on an annual basis. This should be done periodically, as needed.

A "covered account" includes: (i) an account primarily for personal, family, or household purposes, such as a credit card account, mortgage loan, auto loan, checking or savings account that permits multiple payments or transactions, and (ii) any other account that the institution offers or maintains for which there is a reasonable foreseeable risk to customers or the safety and soundness of the institution from identity theft. 717.90(b)(3)

Cell: A11

Comment: Appendix J, Section I states a credit union may incorporate existing policies and procedures that control reasonably foreseeable risks to members or the safety and soundness of the credit union from identity theft. The Red Flags Rule does not require a credit union to develop an all encompassing standalone written Identity Theft Program. Most likely, a credit union will leverage off existing policies and procedures, incorporating those into the written ID Theft Program. If a credit union chooses this option, weaknesses in these other policies and procedures could result in the credit union being in violation of the Red Flags Rule.

Cell: A12

Comment: The Guidelines, Appendix J Section VI(b)(1) recommends the board of directors receive at least annual reports on the compliance of the credit union with the Red Flags Rule.

Cell: A13

Comment: To signal that the final rules are flexible, and allow smaller credit unions to tailor their Programs to their operations, the final rules state that the Program must be appropriate to the size and complexity of the credit union and the nature and scope of its activities.

Cell: A14

Comment: The guidelines are intended to assist credit unions in the formulation and maintenance of a Program that satisfies the requirements of section 717.90. Credit unions must consider the guidelines and include in their Program those guidelines that are appropriate. While a credit union may determine that particular guidelines are not appropriate to include, the Program must nonetheless contain reasonable polices and procedures to meet the specific requirements of the final rule.

Cell: A15

Comment: Credit unions may, but are not required to use the illustrative examples of Red Flags in Supplement A to the Guidelines to identify relevant Red Flags (717.90(d)(2); Appendix J, Sections II, III and IV)

Cell: A16

Comment: The final rule and guidelines do not require the use of any specific technology, systems, processes or methodology.

Cell: A17

Comment: A credit union should periodically conduct a risk assessment to determine whether changes in risks, threats, services, or policies and procedures undermine or weaken the Program's effectiveness.

Cell: A19

Comment: Proper training will enable staff to address the risk of identity theft. However, this provision requires training of only relevant staff. In addition, staff that has already been trained, for example, as a part of the anti-fraud prevention efforts of the credit union, do not need to be retrained except ‘‘as necessary.’’

Cell: A20

Comment: Whenever a credit union engages a service provider to perform an activity in connection with one or more covered accounts the 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 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 credit union, or to take appropriate steps to prevent or mitigate identity theft.

Cell: A22

Comment: The term "credit card" means any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit. The definition of ‘‘debit card’’ is any card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of the consumer at such financial institution for the purposes of transferring money between accounts or obtaining

money, property, labor, or services.

Cell: A23
Comment: The protections of this provision must extend to consumers who hold a card for a personal, household, family or business purpose.

Cell: A24
Comment: Even where the card issuer and cardholder agree to some other means for notice, this alternative means does not change the important nature of the notice and such alternative means does not meet the requirement of the rule (e.g. notice must be separate from regular correspondence). Clear and conspicuous means reasonably understandable and designed to call attention to the nature and significance of the information presented.