PART 681—IDENTITY THEFT RULES

Sec. 681.1 Duties of users of consumer reports regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1) (users).

(b) Definition. For purposes of this section, a notice of address discrepancy means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681m(e), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) Reasonable belief.—(1) Requirement to form a reasonable belief. A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom the user requested the report, when the user receives a notice of address discrepancy.

(2) Examples of reasonable policies and procedures. (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) Consumer's address.—(1) Requirement to furnish consumer's address to a consumer reporting agency. A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report; and

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) Examples of confirmation methods. The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report; and

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) Timing. The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

§ 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) Scope. This section applies to financial institutions and creditors that
are subject to administrative enforce-
ment of the FCRA by the Federal
Trade Commission pursuant to 15
U.S.C. 1681s(a)(1).

(b) Definitions. For purposes of this
section, and appendix A, the following
definitions apply:

(1) **Account** means a continuing rela-
tionship established by a person with a
financial institution or creditor to ob-
tain 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 involv-
ing a deferred payment; and

(ii) A deposit account.

(2) The term **board of directors** in-
cludes:

(i) In the case of a branch or agency
of a foreign bank, the managing offi-
cial in charge of the branch or agency;
and

(ii) In the case of any other creditor
that does not have a board of directors,
a designated employee at the level of
senior management.

(3) **Covered account** means:

(i) An account that a financial insti-
tution or creditor 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, margin account, cell phone ac-
count, utility account, checking ac-
count, or savings account; and

(ii) Any other account that the finan-
cial institution or creditor offers or
maintains for which there is a reason-
ably foreseeable risk to customers or
to the safety and soundness of the fi-
nancial institution or creditor from
identity theft, including financial,
operational, compliance, reputation, or
litigation risks.

(4) **Credit** has the same meaning as in

(5) **Creditor** has the same meaning as
in 15 U.S.C. 1681a(r)(5), and includes
lenders such as banks, finance compa-
ies, automobile dealers, mortgage
brokers, utility companies, and tele-
communications companies.

(6) **Customer** means a person that has
a covered account with a financial in-
stitution or creditor;

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

(8) **Identity theft** has the same mean-
ing as in 16 CFR 603.2(a).

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

(10) **Service provider** means a person
that provides a service directly to the
financial institution or creditor.

(c) **Periodic Identification of Covered
Accounts.** Each financial institution or
creditor must periodically determine
whether it offers or maintains covered
accounts. As a part of this determina-
tion, a financial institution or creditor
must conduct a risk assessment to de-
termine whether it offers or maintains
covered accounts described in para-
graph (b)(3)(ii) of this section, taking
into consideration:

(1) The methods it provides to open
its accounts;

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

(3) Its previous experiences with iden-
tity theft.

(d) **Establishment of an Identity Theft
Prevention Program.**—(1) Program re-
quirement. Each financial institution or
creditor that offers or maintains one or
more covered accounts must develop
and implement a written Identity
Theft Prevention Program (Program)
that is designed to detect, prevent, and
mitigate identity theft in connection
with the opening of a covered account
or any existing covered account. The
Program must be appropriate to the
size and complexity of the financial in-
nstitution or creditor and the nature
and scope of its activities.

(2) **Elements of the Program.** The Pro-
gram must include reasonable policies
and procedures to:

(i) Identify relevant Red Flags for the
covered accounts that the financial in-
nstitution or creditor offers or main-
tains, and incorporate those Red Flags
into its Program;

(ii) Detect Red Flags that have been
incorporated into the Program of the
financial institution or creditor;

(iii) Respond appropriately to any
Red Flags that are detected pursuant
to paragraph (d)(2)(ii) of this section to
prevent and mitigate identity theft; and
(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

c) Administration of the Program. Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

d) Guidelines. Each financial institution or creditor that is required to implement a Program must consider the guidelines in appendix A of this part and include in its Program those guidelines that are appropriate.

§ 681.3 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to a person described in §681.2(a) that issues a debit or credit card (card issuer).

(b) Definitions. For purposes of this section:

(1) Cardholder means a consumer who has been issued a credit or debit card.

(2) Clear and conspicuous means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(3) Address validation requirements. A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer’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. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder’s former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to §681.2 of this part.

(d) Alternative timing of address validation. A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) Form of notice. Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

APPENDIX A TO PART 681—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

Section 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in §681.2(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 financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of §681.2 of this part.