

XYZ FEDERAL CREDIT UNION

FACT ACT POLICY

1) Introduction:

Under the Fair and Accurate Credit Transactions Act – *15 U.S.C. §1681 Et. Seq.* (herein referred to as FACT Act), financial institutions (and creditors) that offer or maintain “covered accounts” must develop and implement a written identity theft prevention program that is appropriately tailored to the size and complexity of the institution, as well as the nature and scope of its activities. The Program requires reasonable policies and procedures, staff training, oversight of service providers, and oversight by the Board of Directors. These rules are set forth in NCUA Rules and Regulations §717.

NCUA Rules and Regulations §717 also require credit and debit card issuers to establish reasonable policies and procedures to assess the validity of a change of address when there is also a request for an additional or replacement card within a short period of time. Likewise, users of consumer reports who receive a notice of an address discrepancy from a Credit Reporting Agency (Herein “CRA”) must have procedures in place in order to form a reasonable belief of the consumer’s identity.

2) Purpose:

The purpose of this policy is to set forth the guidelines for management and staff to use in establishing and maintaining policies and procedures in order to comply with the FACT Act’s guidelines on detecting, preventing and mitigating identity theft.

The policy further addresses the FACT Act’s requirements regarding a card-holder’s request for a replacement card as well as the Act’s requirement for addressing address discrepancies provided by a CRA.

IDENTITY THEFT RED FLAG POLICY

1) Definitions:

a) Account: A continuing relationship established by a person with XYZ Federal Credit Union to obtain a product or service for personal, family, household or business purposes.

i) Business Accounts: Although this definition includes business accounts, the risk-based nature of the final rules allows XYZ Federal Credit Union flexibility to determine which business accounts will be covered by its Program through a risk evaluation process.

- ii) Continuing Relationship: The obligations of the final rule apply not only to existing accounts, where a relationship already has been established, but also to account openings, when a relationship has not yet been established.
- b) Covered Account: Pursuant to §717, we must develop and implement a “written program” if we offer or maintains a “Covered” Account. A “Covered” Account consists of either:
- i) Personal, family, or household purposes: An Account is a “Covered” Account if primarily used for personal, family, or household purposes involving **or** is designed to permit **multiple payments or transactions**; such as
- Credit Card;
 - Mortgage Loan;
 - Automobile Loan;
 - Checking Account;
 - Share Account.
- ii) “Reasonably foreseeable Risk:” A “Covered” Account is any other account for which there is a “reasonably foreseeable risk” to members **or** the safety and soundness of the Credit Union from identity theft. This risk may include financial, operational, compliance, reputation, or litigation risk(s).
- c) Identity Theft: Means a “fraud committed or attempted using the **identifying information** of another person without authority.
- i) Identifying Information: means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:
- Name, SS, DOB, State/Govt. issued DL or identification number, alien registration, EIN, passport;
 - Unique biometric data;
 - Unique electronic identification number, address, or routing code; or
 - Telecommunication identifying information or access device.
- d) Red Flag: means “a pattern, practice, or specific activity that indicates the possible existence of identity theft.”
- e) Service Provider: means “a person that provides a service directly to the Credit Union.”
- 2) Periodic Identification of “Covered” Accounts (Risk Assessment): XYZ Federal Credit Union will periodically determine whether it offers or maintains any covered accounts. As part of this determination, XYZ Federal Credit Union will conduct a risk assessment to determine whether it offers or maintains covered accounts.

a) Risk Assessment Factors: In performing the Risk Assessment we will take the following into consideration:

- Methods the Credit Union provides to open its accounts;
- Method the Credit Union provides to access accounts;
- Prior experience with Identity Theft.

b) Appendix 1: Please refer to Appendix 1 which identifies our “Covered” Accounts.

3) Identity Theft Program: In accordance to the Identity-Theft Regulation, the XYZ Federal Credit Union developed an Identity Theft Program (herein referred to as the “Program”) designed to detect, prevent, and mitigate ID Theft in connection with the opening of a covered account **or** any existing covered account. The elements of the program are as follows:

- Identify Relevant Red Flags;
- Detect Red Flags;
- Respond to detected Red Flags; and
- Update Red Flag program.

a) Identifying relevant Red Flags-Element 1:

i) Goal: Identify **relevant** “Red Flags” for covered accounts. This means we are not required to formulate Red Flags relevant for detecting “possible risk” only “Actual Risk.”

ii) Risk Factors: In identifying relevant Red Flags XYZ Federal Credit Union shall consider the following factors:

- The types of covered accounts offered or maintained;
- The methods provided to open these accounts;
- The methods provided to access covered accounts; and
- Our previous experiences with ID Theft.

iii) Sources of Red Flags: The Credit Union will consider incorporating relevant Red Flags from sources including, but not limited to:

- Our previous incidences with ID Theft;
- Changes in the methods of ID Theft that reflect changes in ID Theft Risk; and
- Applicable supervisory guidance.

iv) Categories of Red Flags: Our Program shall include relevant Red Flags from the following categories:

1) Alerts, notifications, or other warnings received from a CRA or service providers:

The alerts, notifications, or other warnings include, but are not limited to:

- A fraud or activity duty alert is included with a consumer report;
- A CRA provides a notice of credit freeze in response to a request for a consumer report;
- A CRA provides a notice of address discrepancy (see §717.82(b));
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member;

- The credit report or use of the account that indicates a pattern of activity is inconsistent with the history or pattern of activity usually associated with the member, such as:
 - A recent and significant increase in the volume of inquiries;
 - An unusual number of recently established credit relationships;
 - A material change in the use of credit, especially with respect to recently established credit relationships; or
 - An account that was closed for cause or identified for abuse of account privileges by a financial institutions or creditor.

- 2) Presentation of suspicious documents: This may include, but not limited to:
 - Documents provided for identification appear to be forged or altered;
 - The photograph, description of the consumer, or other information on the identification is inconsistent with the appearance of the consumer who is presenting the identification;
 - Other information on the identification is not consistent with the information on the identification provided by the person when the account is opened or by the consumer presenting the identification.;
 - Other information provided is inconsistent with information on file with First Financial, such as a signature card or recent check; or
 - An application appears to be altered, or destroyed and reassembled.

- 3) Presentation of suspicious personal identifying information, such as a suspicious address change: This may include, but is not limited to:
 - Personal information provided is inconsistent when compared to external information sources, such as:
 - The address does not match any address in the credit report; or
 - The SSN has not been issued, or is listed on the Social Security Administration's Death Master File.
 - Personal information is internally inconsistent, such as an SSN that is inconsistent with a consumer's date of birth;
 - Personal information is provided that has also been provided on a fraudulent application;
 - Personal information that is provided is of a type associated with fraudulent activity, such as a fictitious address (i.e., mail drop or a prison) and an invalid phone number (i.e., pager or answering service);
 - The address, SSN, and phone numbers have been submitted by other consumers;
 - The consumer fails to provide all required information on an application;
 - Personal information is not consistent with information on file with the Credit Union; or
 - The consumer cannot provide authenticating information, other than what would be available from a wallet or credit report.

4) The unusual use of, or other suspicious activity related to, a covered account: This may include, but is not limited to:

- There is a request for additional authorized users for the account or a request for new, additional, or replacement cards shortly after a request for a change of address;
- A new, revolving credit account is used in a manner associated with fraud, such as credit used for cash advances or for merchandise that is easily converted to cash, or the member fails to make payments;
- An account is used in a manner inconsistent with established patterns of activity, such as:
 - Nonpayment when there is no history of late or missed payments;
 - A material increase in the use of available credit;
 - A material change in purchasing or spending patterns;
 - A material change in electronic fund transfer patterns in connection with a deposit account; or
 - A material change in telephone call patterns in connection with a cellular phone account.
- An 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);
- Mail sent to the member is returned repeatedly as undeliverable even though transactions on the account continue to be conducted;
- XYZ Federal Credit Union is notified that the member is not receiving paper account statements;
- XYZ Federal Credit Union is notified of unauthorized charges or transactions in connection with the account;
- XYZ Federal Credit Union has been notified that it has opened a fraudulent account for a person engaged in identity theft.

5) Notice from members, ID Theft victims, law enforcement, or other persons regarding possible ID Theft: The Credit Union is notified by a:

- Member;
- Victim of ID Theft;
- Law Enforcement Authority; or
- Any other person that it has opened a fraudulent account for a person **engaged in** ID Theft.

b) Detecting Red Flags- Element 2: The Credit Union shall apply procedures and processes in detecting Red Flags in connection with the opening of covered accounts and existing covered account, such as:

- i) Opening of Covered Account: The Credit Union shall cross reference other operating policies and procedures for obtaining identifying information about, and verifying the identity of, a person opening a covered account such as our Customer Identification Program (CIP);

ii) Existing Covered Accounts: The Credit Union shall cross reference the detection of Red Flags in connection with existing covered accounts by Authenticating Members (See **§748 Security Program**); Monitoring Transactions (See **BSA/AML Transaction Structuring**); and Validating Change of Address (See **717.82**).

c) Respond to detected Red Flags- Element 3: The Credit Union shall respond appropriately upon the detection of Red Flags. Appropriate responses may include the following:

- Monitoring a “covered account” for evidence of Identity Theft;
- Contacting the Member;
- Changing any password, security codes, or other security devices;
- Reopening a covered account with a new account number;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstance(s).

d) Updating the Program- Element 4: The Credit Union shall periodically update the program to reflect changes in risk to members **or** safety/soundness of the Credit Union, based on factors such as:

- Experience with Identity Theft;
- Changes in methods of Identity Theft;
- Changes in methods to detect, prevent, and mitigate Identity Theft;
- Changes in types of accounts Credit Union offers; and
- Changes in business arrangements of the Credit Union, including mergers, acquisitions, alliances, and service provider arrangements.

4) Administration of the Program: Administration of the Program shall consist of the following components:

a) Board of Director/Senior Management Involvement: The Board or an appropriate committee of the Board shall approve the initial written Program. Thereafter, at the discretion of XYZ Federal Credit Union Board of Directors, Senior management may update the Program. Oversight will include the following:

i) Assigning specific responsibility for the program’s implementation;

ii) Reviewing annual reports prepared by staff regarding compliance with the Red Flags rules. The report will address the following matters related to the Program:

- 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; and

iii) Approving material changes to the Program, as necessary, to address changing identity theft risks.

b) Oversight of service provider(s): Whenever the Credit Union engages a service provider to perform an activity in connection with one or more covered accounts the Credit Union shall take steps to ensure the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of ID Theft.

XYZ shall satisfy this requirement through our Third Party Vendor Due Diligence Program (TPDD). The TPDD program includes reviewing financial and organizational infrastructure of the vendor. The TPDD also includes a review of the vendor's contract to ensure the vendor has policies and procedures to detect relevant Red Flags.

c) Training: "Relevant Staff" shall receive training to effectively implement and administer the Program. "Relevant Staff" is not defined in the regulation nor comments thereto.

However, we consider the following as "relevant" in complying with the ID Theft regulation:

- CEO;
- VP of Operations;
- Teller Area;
- MSR Area;
- Lending staff.

5) Other Applicable Legal Requirements: In complying with the Identity-Theft Regulations, XYZ shall be mindful of other related legal requirements including:

- Filing Suspicious Activity Reports (SARs);
- Implementing requirements under the FACT Act regarding the circumstances under which credit may be extended when fraud or an active duty alert is detected;
- Implementing requirements under the FACT Act of furnishers of information to CRAs to correct or update inaccurate or incomplete information and not to report information that the furnisher reasonably believes is inaccurate; and
- Complying with FACT Act prohibitions against the sale, transfer, and placement for collection of certain debts resulting from identity theft.

CARD-HOLDER'S REQUEST FOR REPLACEMENT CARD

1) Purpose: Validate a change in address for a debit/credit card with a "recent" request for a replacement card.

- Recent Request: 30 days;
- What about simply a Request for Replacement Card?: No need to validate if only a request for replacement card.
- What if request > 30 days: No need to validate. However, the Credit Union reserves the right to apply procedures identified in section 3 below.

- 2) Applicability: These rules apply only to:
- Personal, household, family, or business purposes;
 - Debit, Credit, Payroll, or Home Equity if accessible through a credit/debit card;
 - Not covered: Gift cards or other prepaid cards.
- 3) Procedures for issuing replacement card: The Credit Union will not issue an additional or replacement credit or debit card if such a request is received within a short period of time after receiving notification of a change of address for that account unless the Credit Union does the following:

Method 1:

- i) Notifies Cardholder: of the request
- 1) Former Address: Notifying cardholder at former address; or
 - 2) Other agreed-upon means: Notifying cardholder by any other means both parties previously agreed upon. **And**
- ii) Provide cardholder reasonable means of promptly reporting incorrect address change.

Method 2:

- i) Apply Red Flag Procedures: As set forth in the Identity Theft Red Flag section above.

- 4) Notice Requirements: Any written or electronic notice provided under this policy will be “Clear and Conspicuous” and provided separately from the regular correspondence that is sent to the member. “Clear and Conspicuous” is defined as “reasonably understandable and designed to call attention to the nature and significance of the information.”

DUTIES OF USERS OF CONSUMER REPORTS REGARDING ADDRESS DISCREPANCIES

- 1) Purpose: Enhance accuracy of consumer information and to ensure the Credit Union obtains the correct consumer report on the consumer whom it requested the report.
- 2) Duties:
- CRA: CRA must provide Credit Union notice of existence of address discrepancy if address provided by Credit Union “substantially differs” from what the CRA has on file;
 - Credit Union (user): Credit Union must develop policies and procedures to handle receipt of notice of discrepancy from a CRA.
- 3) Program Components: In accordance to the regulation, our procedures shall consist of three (3) elements:
- Formation of “Reasonable Belief;”
 - Furnishing address to CRA; and
 - Submitting Confirmation to CRA.

a) Procedures to handle receipt of notice of address discrepancy from a CRA- **Element 1**: The Credit Union shall form a “Reasonable Belief” that a consumer report relates to the member about whom it has requested to report. As a user of consumer report information, XYZ Federal Credit Union will perform the following when in receipt of a notice of address discrepancy from a CRA:

- i) Utilize Credit Union data: The Credit Union will compare information in the consumer report provided by the CRA against Credit Union data, including but not limited to:
- CIP Information: New Accounts only (not existing);
 - “In-House” records: such as loan applications, internal change of address forms;
 - Third-Party Resources: Collection reports, etc.

Or

- ii) Consumer Verification: Credit Union should verify address discrepancy directly with member.

b) Furnishing Address to CRA- **Element 2**: The Credit Union will also use reasonable procedures for address validation to the CRA from which it received a notice of address discrepancy when the Credit Union:

- i) Reasonable Belief: The Credit Union can form a reasonable belief that the report relates to the member about whom the Credit Union requested the report;

- ii) Continuing Relationship: The Credit Union establishes a “continuing relationship” with the member; **and**

- iii) Ordinary Course of Business: The Credit Union regularly, and in the ordinary course of business, furnishes information to the CRA from which the notice of address discrepancy was obtained.

- iv) Acceptable Methods of Confirmation: The Credit Union may reasonably validate the accuracy of an address by any of the following methods:

- 1) Consumer Verification: Verify information with member;
- 2) Third-Party: Verify address with third party; or
- 3) Other “Reasonable Means.” The Credit Union may employ other reasonable procedures to confirm the accuracy of the address. This is at the discretion of the Credit Union.

c) Timely Submission of member’s address to CRA- **Element 3**: The Credit Union shall provide the member’s **validated** address to the CRA as part of the information the Credit Union regularly furnishes to the CRA.

Reviewed and Approved by Board of Directors:

Date: _____