

# Eastpointe Community Credit Union Identity Theft and Deterrence Policy

Areas of Responsibility: Management/Operations  
Board Approval: October 15, 2008  
Board Review: (enter BOD review date)  
Last Revision: Leave blank if not applicable

## Introduction:

Under the Fair and Accurate Credit Transactions Act (FACT Act), financial institutions (and creditors) that offer or maintain "covered accounts" (defined below) must develop and implement a written identity theft prevention program (the Program) that is appropriate 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.

The rules 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. Users of consumer reports who receive a notice of an address discrepancy from a credit bureau must have procedures in place in order to form a reasonable belief of the consumer's identity.

## General Policy Statement:

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.

### 1) DEFINITIONS:

- A) Account: A continuing relationship established by a person with Eastpointe Community Credit Union to obtain a product or service for personal, family, household or business purposes.
  - i) Although this definition includes business accounts, the risk-based nature of the final rules allows the Credit Union flexibility to determine which business accounts will be covered by its Program through a risk evaluation process.
  - ii) 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: An account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or
- i) 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, including financial, operational, compliance, reputation or litigation risks.
- C) Identity Theft: A fraud committed or attempted using the identifying information of another person without authority. The Federal Trade Commission (FTC) defines the term "identifying information" to mean, "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any of the following:
- i) Name, Social Security Number (SSN), date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
  - ii) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
  - iii) Unique electronic identification number, address or routing code; or
  - iv) Telecommunication identifying information or access device.
- D) Red Flag: A pattern, practice or specific activity that indicates the possible existence of identity theft.
- E) Service Provider: A person that provides a service directly to the Credit Union.

## 2) IDENTIFICATION OF COVERED ACCOUNTS:

- A) The Credit Union will periodically determine whether it offers or maintains any covered accounts. As part of this determination, the Credit Union takes the following into consideration: The methods it provides to open its accounts; the methods it provides to access its accounts; and its previous experience with identity theft.
- i) All accounts offered by Eastpointe Community Credit Union are covered accounts as defined in Section 1 (B). All accounts that the Credit Union offers, and the methods allowed for opening and accessing accounts create some risk and the potential for identity theft. It is imperative that Eastpointe Community Credit Union take a proactive position on preventing identity theft of its members. This program is designed to offer such an approach.
- B) The Credit Union offers a wide variety of services and accounts to its members. Basic accounts include, but are not limited to:

- Savings Accounts
- Checking Accounts
- CD's
- Christmas Club Accounts
- 
- Individual Retirement Accounts
- Equity Loans)
- Secured Loans
- Unsecured Loans
- Other Lines of Credit (LOCs)

- C) Account Opening Methods: There are various ways of opening accounts with the Credit Union, which include, but are not limited to:
- i) In person
  - ii) Over the phone (if existing membership relationship)
  - iii) Remotely (through approved indirect dealers)
  - iv) Mail

- D) Account Access Methods: Members may access their accounts in the following ways (this list is not comprehensive):

- Wire Transfers
- ACH Transfers
- Mail
- Convenience Checks
- Interactive Telephone Banking
- Credit Cards
- Debit Cards
- Sale of Monetary Instruments
- Check Cashing
- Phone (with staff assistance)
- Overdraft Protection
- Internet Banking
- On-line Bill Pay
- Pre-paid Gift Cards

- E) FFCU Identity Theft: The credit union has experienced very little identity theft.
- i) No known instances of identity theft at account opening
  - ii) No known instances of fraudulent address changes
  - iii) The credit union has experienced identity theft through a service provider; however no known fraud was committed
  - iv) In our experience the majority of identity theft experienced by FFCU is perpetrated by family members

### 3) DEVELOPMENT AND IMPLEMENTATION OF IDENTITY THEFT PREVENTION PROGRAM

- A) IDENTIFICATION OF RED FLAGS: In determining which Red Flags may be relevant to the development of the program, the following factors will be considered:
- i) The types of covered accounts offered or maintained;
  - ii) The methods provided to open these accounts;
  - iii) The methods provided to access covered accounts; and
  - iv) Previous experiences with identity theft.
  - v) The relevant Red Flags will be incorporated from the following sources:
  - vi) Previous experiences with identity theft;
  - vii) Changes in the methods of identity theft that reflect changes in the risk; and
  - viii) Applicable supervisory guidance.

- B) RED FLAGS: As part of its identity theft prevention program, the Credit Union has determined the following Red Flags will apply and should be included in the Identity Theft Prevention Program. The credit union will develop procedures to monitor activity for the detection of the following Red Flags. The Credit Union will periodically update this list as new experiences are encountered.
- i) A fraud or active duty alert is included with the credit report.
  - ii) A credit bureau provides a notice of a credit freeze in response to a request for a credit report.
  - iii) A credit bureau provides a notice of address discrepancy.
  - iv) 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:
    - (1) A recent and significant increase in the volume of inquiries;
    - (2) An unusual number of recently established credit relationships;
    - (3) A material change in the use of credit, especially with respect to recently established credit relationships; or
    - (4) An account that was closed for cause or identified for abuse of account privileges by a financial institutions or creditor.
  - v) Documents provided for identification appear to be forged or altered.
  - vi) 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.
  - vii) 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.
  - viii) Other information provided is inconsistent with information on file with the Credit Union, such as a signature card or recent check.
  - ix) An application appears to be altered, or destroyed and reassembled.
  - x) Personal information provided is inconsistent when compared to external information sources, such as:
    - (1) The address does not match any address in the credit report; or
    - (2) The SSN has not been issued, or is listed on the Social Security Administration's Death Master File.
  - xi) Personal information is internally inconsistent, such as an SSN that is inconsistent with a consumer's date of birth.
  - xii) Personal information is provided that has also been provided on a fraudulent application.
  - xiii) 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).
  - xiv) The address, SSN, and phone numbers have been submitted by other consumers.
  - xv) The consumer fails to provide all required information on an application.
  - xvi) Personal information is not consistent with information on file with the Credit Union.
  - xvii) The consumer cannot provide authenticating information, other than what would be available from a wallet or credit report.
  - xviii) 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.
  - xix) 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.

- xx) An account is used in a manner inconsistent with established patterns of activity, such as:
  - (1) Nonpayment when there is no history of late or missed payments;
  - (2) A material increase in the use of available credit;
  - (3) A material change in purchasing or spending patterns;
  - (4) A material change in electronic fund transfer patterns in connection with a deposit account; or;
  - (5) A material change in telephone call patterns in connection with a cellular phone account.
- xxi) 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).
- xxii) Mail sent to the member is returned repeatedly as undeliverable even though transactions on the account continue to be conducted.
- xxiii) The Credit Union is notified that the member is not receiving paper account statements.
- xxiv) The Credit Union is notified of unauthorized charges or transactions in connection with the account.
- xxv) The Credit Union has been notified that it has opened a fraudulent account for a person engaged in identity theft.

C) Detection of and Response to Red Flags:

- i) Detection: The Credit Union will address the Red Flags in connection with the opening of covered accounts by obtaining and verifying information about the identity of a person opening a covered account (for example, by using the existing CIP rules set forth in the Bank Secrecy Act). The Credit Union will address the detection of Red Flags in connection with existing covered accounts by authenticating members, monitoring transactions, and verifying the validity of change of address requests.
- ii) Responding: In order to respond appropriately, the Credit Union will assess whether the Red Flag detected evidence a risk of identity theft, and will have a reasonable basis for concluding that a Red Flag does not evidence such a risk.

D) Updating the Program: The Credit Union will periodically update its policies, procedures and risk assessment to reflect changes in identity theft risks to members and to the safety and soundness of the Credit Union.

- i) Additionally, this program may be modified:
  - (1) As new products and services are added
  - (2) If at any time, any portion proves counterproductive to the policy's intent of preventing and detecting identity theft
  - (3) As trends in identity theft change
  - (4) If the Credit Union sees a dramatic increase in the occurrences of identity theft or sees in an increase in the number of red flags
  - (5) As the Credit Union's experience with identity theft becomes more in-depth

#### 4) ADMINISTRATION OF THE PROGRAM

- A) Involvement of the Board of Directors and Senior Management: The Board will approve the initial written policy. Thereafter, at the discretion of the Board, Senior Management may update the Program. Board of Directors and Senior Management oversight will include the following:
- i) The Compliance Officer is appointed to be specifically responsible 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:
  - iii) 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;
  - iv) Service provider arrangements;
  - v) Significant incidents of identity theft and management's response to these incidents; and
  - vi) Recommendations for material changes to the Program; and
  - vii) Approving material changes to the Program, as necessary, to address changing identity theft risks.
- B) Training: Identity theft training shall occur at least annually for all credit union employees, officers, and directors.
- C) Service Provider Oversight: If a service provider is used in connection with covered accounts, the Credit Union will ensure that the activity of the service provider is conducted in accordance with FFCU policies and procedures that are designed to detect, prevent and mitigate the risk of identity theft.
- i) The Compliance Officer is responsible for oversight and due diligence of all third parties used in the program. Additionally, the Compliance Officer will report annually to the Board of Directors on:
    - (1) the program's viability and effectiveness
    - (2) service providers being utilized
    - (3) any major occurrences of identity theft and management's response
    - (4) recommendations for changes to the program, if any
- D) Other Applicable Legal Requirements: The Credit Union will follow other applicable legal requirements, such as:
- i) The requirement to file a Suspicious Activity Report;
  - ii) The requirements under the Fair Credit Reporting Act (FCRA) regarding the circumstances under which credit may be extended when fraud or an active duty alert is detected;
  - iii) The requirements under the FCRA of furnishers of information to credit bureaus to correct or update inaccurate or incomplete information, and not to report information that the furnisher reasonably believes is inaccurate; and
  - iv) The FCRA prohibitions against the sale, transfer and placement for collection of certain debts resulting from identity theft.

## 5) USE OF CREDIT REPORTS REGARDING ADDRESS DISCREPANCIES

- A) As a user of credit report information the Credit Union will do the following:
  - i) Compare the information in the credit report provided by the credit bureau with the information that the Credit Union:
    - (1) Obtains and uses to verify the member's identity in accordance with the CIP rules under the Patriot Act;
    - (2) Maintains in its own records, such as applications, change of address notifications, other member account records, or retained CIP documentation; or
    - (3) Obtains from third-party sources.
  - ii) Verify the information in the credit report provided by the credit bureau.
- B) The Credit Union will also use reasonable procedures for furnishing to the credit bureau, from which it received a notice of address discrepancy, when the Credit Union:
  - i) Can form a reasonable belief that the report relates to the member about whom the report was requested;
  - ii) Establishes a continuing relationship with the member; and
  - iii) Regularly and in the ordinary course of business furnishes information to the credit bureau from which the notice of address discrepancy was obtained.
- C) The Credit Union may reasonably confirm that an address is accurate by any of the following methods:
  - i) Verifying the address with the member;
  - ii) Reviewing its own records to verify the address of the member;
  - iii) Verifying the address through third party sources; or
  - iv) Using other reasonable means.
- D) The Credit Union will provide the member's address (that 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 member.

## 6) EASTPOINTE COMMUNITY CREDIT UNION PROCEDURES:

The following section outlines the procedures Eastpointe Community Credit Union will employ to help prevent identity theft when red flags are present.

The greatest tool in the Credit Union's arsenal to combat identity theft is E-Funds OFAC and ID Verification Solutions. It is the practice of Eastpointe Community Credit Union to verify all identification presented at account opening through E-Funds ID Verification Solution. ID Verification returns a "Pass" or "Fail" for the identification presented. All Member Service Representatives must either (a) receive a "Pass" notification prior to opening a new account; or (b) obtain additional identifying information if the ID Verification Solution returns a "Fail" response. Additional verification methods must be documented in account notes, and provide reasonable evidence that an override for the "Fail" notification is warranted. If additional verification cannot be obtained, then the account may not be opened.

- A) Common Practices for Identity Theft Prevention: The "Common Practices" section is designed to offer an overall holistic approach to the prevention of identity theft. These practices are implemented enterprise wide and applicable to all departments and persons employed by the credit union.
- B) Use of Document Control Practices: All paper documentation produced by the credit union or provided by members shall be filed under lock and key, imaged and then destroyed, or immediately destroyed depending upon business need. Documentation containing any member information shall not be left unattended on desks or workstations, and shall not be left unsecured overnight. The credit union uses multiple tools in an effort to move to a "paperless" atmosphere, including e-faxing, direct document imaging, and daily shredding of material containing member information, which is not being retained or imaged.
- C) Management of non-Credit Union Personnel While on Credit Union Property: With limited exception, all non-credit union personnel must be escorted by a Credit Union employee or designee while on Credit Union premises. This includes, but is not limited to vendors and business partners, maintenance and repair personnel, delivery personnel, visitors, or any other person not employed by the Credit Union. Non-credit union personnel will be required to sign in to the visitor's log book, and must wear a Credit Union provided Visitor's pass somewhere on their person. Non-credit union personnel are generally not permitted to access restricted areas of the Credit Union.
- D) Employee acknowledgement of the Credit Union's Identity Theft Prevention Program: All credit union employees shall be required to sign an acknowledgement form indicating that they have received a copy of this policy, or know where to find it; that they are aware of their role in preventing identity theft; they understand the consequences of failure to comply with the provisions of this policy; and that they have received training regarding the implementation of this policy and its procedures.

**7) Information from a Consumer Reporting Agency:**

*Since the Credit Union relies heavily on the use of Consumer Credit Reports, it is imperative that these red flags are identified and addressed immediately.*

- A) If a fraud or active duty alert, or a notice of credit freeze is included within a consumer report, then one or more of the following will occur:
  - i) The Credit Union Employee will follow the direction outlined within the alert (i.e. If the alert states to call the consumer before extending credit, then we will do so).
  - ii) We will obtain additional identification to ensure that we are dealing with the actual member/consumer.
  - iii) We will ask the member/consumer "out of wallet" questions about information contained in the credit report.

- B) If a notice of address discrepancy is provided by a consumer reporting agency, then one or more of the following will occur:
- i) We will refer to the results of our E-Funds ID Verification results and ensure that we received a "Pass" for the address verification.
  - ii) We may require additional documentation to verify the member/consumer's address, such as a utility bill, lease agreement or other documentation that meet's the Credit Union's standards.
  - iii) We will notify the credit reporting agency of the address discrepancy, and provide them with the correct/updated address.
- C) If a consumer credit 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 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; An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor, then one or more of the following will occur:
- i) We may refuse to open another account or establish a relationship with the consumer/member.
  - ii) We will refer to the results of our E-Funds ID Verification results and ensure a "Pass" status for all sections.
  - iii) We may ask for additional documentation or identification to the extent that we are satisfied that the person requesting credit and the person's credit profile are one in the same.
  - iv) If an account is established, the Credit Union has the right to categorize the account as a high risk account and monitor the account until we are comfortable with the performance of the account.
- D) Documentary Information:
- i) If documents provided for identification appear to have been altered, then one or more of the following will occur:
    - (1) The ID or documentation presented may be subjected to black light testing to ensure validity, or a Credit Union employee will refer to the 2008 ID Checking Guide found in all branches.
    - (2) We may ask the consumer/member for additional identification.
    - (3) We may refuse to conduct the requested transaction or establish a relationship for the member/consumer.
  - ii) If the photograph or physical description on the identification is not consistent with the appearance of the applicant presenting the identification, then one or more of the following will occur:
    - (1) The ID or documentation presented may be subjected to black light testing to ensure validity, or a Credit Union employee will refer to the 2008 ID Checking Guide found in all branches.
    - (2) We may ask the member/consumer for additional identification.
    - (3) We may refuse to conduct the requested transaction or establish a relationship for the member/consumer.

- iii) If other information on the identification is not consistent with information provided by the person presenting the identification, or is not consistent with information that is on file, such as a signature card, then one or more of the following will occur:
  - (1) The ID or documentation presented may be subjected to black light testing to ensure validity, or a Credit Union employee will refer to the 2008 ID Checking Guide found in all branches.
  - (2) We may ask the consumer/member for additional identification; to the extent that we are satisfied that true identification has been obtained.
  - (3) We may refuse to conduct the requested transaction or establish a relationship for the member/consumer.

E) Personal Information:

- i) If personal information provided is inconsistent when compared against external information sources (E-Funds ID Verification Solution, or the Social Security Number has not been issued, or is listed on the Social Security Administration's Master Death File); or if personal information provided is internally inconsistent (e.g.: there is a lack of correlation between the SSN range and the applicant's date of birth); then one or more of the following will occur:
  - (1) We may ask the applicant/member to provide a letter from the Social Security Administration verifying the validity of the social security number being presented.
  - (2) We may refuse to conduct the requested transaction or establish a relationship for the member/consumer.
  - (3) We may, at our discretion, use any other means at our disposal to investigate the validity of the social security number being presented.
- ii) If personal information provided is a type commonly associated with fraudulent activity, such as an address on an application is fictitious, a mail drop, or a prison; or the phone number provided is invalid, or is associated with a pager or answering service, then one or more of the following will occur:
  - (1) We may ask the applicant/member for an alternative address that can be verified.
  - (2) We may ask the applicant/member for an alternative phone number that can be verified through independent testing, such as a reverse phone search through the internet.
  - (3) We may refuse to conduct the requested transaction or establish a relationship for the member/consumer.
- iii) If personal information provided is associated with known fraudulent activity; or if the address, SSN, or home or cell number provided is the same as that submitted by other persons opening an account, or if the person opening the account fails to provide all required information on the application; or if the personal information provided is inconsistent with information that is on file; or if the person opening the account or the consumer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report, then one or more of the following will occur:
  - (1) The account will not be opened without management approval.
  - (2) If fraud is suspected the situation will be investigated by the compliance officer or VP of Operations. Investigation results will be documented, and if warranted the appropriate authorities may be notified of the outcome.

- F) Change of Address/Personal Information:
- i) The Credit Union recognizes that invalid address, phone number or email changes requested by fraudsters are a key component in perpetrating identity theft, and as such has established strict procedures for verifying address/personal information changes and monitoring account activity following an address change.
    - (1) Address changes will be accepted in person, by mail, fax, and through the secure messaging system in the online banking system.
    - (2) If the member's information is updated or changed in any way, the Credit Union employee processing the transaction is responsible for obtaining sufficient identification to ensure that we are dealing directly with the authorized account holder.
    - (3) The credit union will send notification of all address/personal information changes not made in person to the previous address on file for address changes and to the current address on file for personal information changes. The notification will provide the member with a phone number to contact the credit union in case of unauthorized changes.
    - (4) A thirty (30) day warning code will be placed on the member's account following a request for an address change.
  - ii) If shortly following a change of address for a member's account, the Credit Union receives a request for a new, additional or replacement debit or credit card, convenience checks, then one or more of the following may occur:
    - (1) The Credit Union will determine if the address/personal information change was completed in person. If the change was completed in person the request will be approved.
    - (2) The Credit Union will not honor the request until the member's identity has been validated, and documentation of such validation has been recorded and made part of the member's file. It is also the general policy of the Credit Union to not honor such requests without management approval.
  - iii) If mail sent to a member is returned as undeliverable although transactions continue to be conducted in connection with the members account, then one or more of the following will occur:
    - (1) A warning code will be placed on the member's account, indicating that we have received mail returned as undeliverable. Mailing of credit union correspondence is restricted and access to the accounts will be restricted until a valid address change is submitted. The next time the member attempts to conduct a transaction at the Credit Union, an override will be required, and the member will be asked for updated information.
- G) Anomalous Use of the Account:
- i) The Credit Union issues both debit and credit cards. For debit cards, we issue a MasterCard and our service provider is CO-OP Network. For credit cards we issue a Visa, and our service provider is CU Card Services/Certegy.
    - (1) For debit cards, when anomalous or unusual activity is detected, our service provider CO-OP Network is responsible for identifying the unusual activity and contacting the member for verification of the transaction. If CO-OP Network is unable to contact the member, and they deem that there is a high risk for potential fraud, the card will be suspended. After the card is suspended, the member must contact the Credit Union. The credit union will determine if the block can be lifted or if re-issuance of a new card is required.

- (2) For credit cards, when anomalous or unusual activity is detected, our service provider CU Card Services/Certegy is responsible for identifying the unusual activity and contacting the member for verification of the transaction. If CU Card Services/Certegy is unable to contact the member, and they deem that there is a high risk for potential fraud, the card will be suspended. After the card is suspended, the member must contact the Credit Union. The credit union will determine if the block can be lifted or if re-issuance of a new card is required.
  - ii) If a new credit card account is used in a manner commonly associated with fraud, for example when the majority of available credit is used for cash advances or merchandise that is easily convertible to cash; or the member fails to make the first payment, or makes the initial payment but no subsequent payments, then one or more of the following will occur:
    - (1) CU Card Services/Certegy will attempt to contact the member to verify the activity. If the member is contacted and the activity is verified, then no further action needs to be taken.
    - (2) If the member cannot be contacted to verify the transaction, then the card may be suspended, depending upon our determination and whether or not we believe there is a potential for fraud.
  - iii) If an account that has been inactive (dormant) for one year or more, then the following will occur:
    - (1) The system will notify the teller that the account is dormant the teller will request identification from the member. The teller will verify that information from the ID matches what is on our system.
    - (2) If the ID presented does not match the information on file for the member, the teller will refuse the transaction or seek a supervisor override.
- H) Notice from Members or Others Regarding Member Accounts:
- i) If Eastpointe Community Credit Union is notified of unauthorized charges in connection with a member's account, then one or more of the following will occur:
    - (1) A Credit Union employee may freeze or close the member's account at their request. The credit union reserves the right to close a compromised account in order to protect the credit union.
    - (2) A Credit Union employee will assist the member in preparing fraud affidavit forms and help the member through the submission process.
    - (3) If warranted, the case may be referred to the Security Committee for further investigation.
  - ii) If Eastpointe Community Credit Union is notified that it has opened a fraudulent account for a person engaged in identity theft, then one or more of the following will occur:
    - (1) The account(s) in question will be immediately frozen or closed.
    - (2) The matter will be referred to the Compliance Officer.
    - (3) A Suspicious Activity Report (SAR) will be filed.
    - (4) The Credit Union will take any additional steps appropriate to protect itself and its member from further loss or exposure.
    - (5) The Credit Union will file a report with the appropriate authorities and pursue all legal channels against the party involved with the identity theft.

- iii) If the Credit Union is notified that the member is not receiving account statements, then one or more of the following will occur:
  - (1) We will attempt to identify the cause of the problem (non-delivery of the statements to the member), and if it is an internal technical problem, we will resolve the problem in a timely manner and ensure that the member begins receiving statements.
  - (2) If the member is not receiving statements due to an incorrect address on file, we will request the member to complete an address change request and correct the address in our system so that the member may begin receiving statements. If we have reason to believe that the member's account information may have been compromised, or at the member's request, we may close the existing account and re-open a new account for the member.
- iv) If the Credit Union is notified that our member may have provided information to someone fraudulently claiming to represent FFCU, or if the member is a victim of a phishing scam that may have compromised account information, user identification, or a personal identification number (PIN) or password, then one or more of the following will occur:
  - (1) Depending upon the sensitivity and amount of information that was inadvertently released by the member to non-Credit Union personnel, we may take or recommend the member take the following actions:
    - (a) Freeze or close the existing account and re-open a new account
    - (b) Obtain a new personal identification number (PIN)
    - (c) Change user identification and/or password(s)
    - (d) Cancel and re-issue a debit or credit card
- I) Other Red Flags:
  - i) If the name of an employee of the Credit Union has been added as an authorized user on an account, then the following will occur:
    - (1) If it is determined that the Credit Union employee added (or had someone to add) his or her name to a member's account without authorization from that member, then the matter will be referred to the VP of Operations.
    - (2) The offending employee(s) will face disciplinary action up to and including termination.
  - ii) If a Credit Union employee accesses or downloads an unusually large number of member account records, then the following will occur:
    - (1) The matter will be investigated internally by the Credit Union's IT department, Compliance Manager, and VP of Operations.
  - iii) If the Credit Union detects or is informed of unauthorized access to a member's personal information, then one or more of the following will occur:
    - (1) An investigative team consisting of the Compliance Officer, IT Manager and the VP of Operations will be formed. The team will investigate how and why a member's personal information was compromised.
      - (a) The investigative team will be responsible for identifying the cause of the unauthorized access, as well as developing an action plan for preventing future occurrences.
      - (b) If the Credit Union is at fault for the loss of, or negligent in the handling of the member's identifying personal information, all reasonable necessary steps needed to further protect the member's identity will be taken by the Credit Union.
      - (c) The member's existing accounts, including debit and credit cards, will be frozen or suspended, and a new account will be established for the member.

- (d) If the results of the investigation reveal internal security breaches, then the offending employees will face disciplinary action, up to and including termination.
- iv) If there are unusually large or frequent check orders in connection with a member's account, then one or more of the following may occur:
  - (1) We will consider the member's previous check ordering history.
  - (2) We may contact the member directly at the phone number in our records to verify the validity of the check order.
  - (3) If there is concern that the member may be using the large amount of checks for any illicit purpose, the matter will be referred to the Compliance Manager for further investigation.
- v) If the person opening an account or a member is unable to lift a credit freeze placed on his or her consumer report, then the following will occur:
  - (1) The Credit Union will not open another account or establish a relationship with the member or consumer until the credit freeze is lifted. No exceptions.