

ClaimAid Self-Pay Solutions
Identity Theft Prevention Program
(Policy guidelines provided by ACA International)

Purpose: To establish an Identity Theft Prevention Program (“Program”) designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide continued administration of the program in compliance with 16 C.F.R. Part 681.

This Program enables ClaimAid Self-Pay Solutions to protect existing consumers, reduce risk from identity fraud, and minimize potential damage to ClaimAid Self-Pay Solutions. The Program will help ClaimAid Self-Pay Solutions:

- A. Identify risks that signify potential fraudulent activity within a new or existing covered account.
- B. Detect risks when they occur in covered accounts.
- C. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed.
- D. Update the Program periodically, including reviewing the accounts that are covered and the identified risks that are part of the Program.

Scope: This Program applies to employees, contractors, consultants, temporary workers, and service providers, including all personnel affiliated with third parties.

Definitions:

- A. **Identity Theft** means fraud committed or attempted using the identifying information of another person without authority. All three of the following must be present for Identity Theft to have occurred:
 - i. Fraud committed or attempted.
 - ii. Using the identifying information of another person.
 - iii. Without authority.
- B. A **covered account** means
 - i. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, auto loans, cell phone accounts, utility accounts; and
 - ii. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
- C. A **red flag** is a pattern, practice, warning sign, or specific activity that indicates the possible existence of identity theft.
- D. **Personally identifiable information** includes the following items whether stored in electronic or printed format:
 - i. Consumer’s
 - a. First, middle, or last name
 - b. Date of birth
 - c. Address
 - d. Telephone or wireless numbers
 - e. Social Security number
 - f. Government-issued identification number
 - g. Maiden name
 - h. Account number

- ii. Credit Card information, including any of the following:
 - a. Credit card number (in whole or in part)
 - b. Credit card expiration date
 - c. Cardholder name
 - d. Cardholder address
- iii. Medical information for any customer, including but not limited to:
 - a. Doctor names and claims
 - b. Insurance claims
 - c. Prescriptions
 - d. Treatment or diagnoses
 - e. Any related personal medical information

The Program

ClaimAid Self-Pay Solutions establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The program shall include reasonable policies and procedures to:

- A. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program.
- B. Detect red flags that have been incorporated into the Program.
- C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
- D. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of ClaimAid Self-Pay Solutions from identity theft.
- E. Development, implementation, continued administration, and operational responsibility of The Program is delegated to the VP of Operations.

Identification of Relevant Red Flags

- A. The Program shall include relevant red flags from the following categories, as appropriate:
 - i. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, including:
 - a. A fraud or activity duty alert included with a consumer report.
 - b. Notices of a credit freeze from a consumer-reporting agency in response to a request for a consumer report.
 - c. A notice of address discrepancy from a consumer-reporting agency.
 - ii. The presentation of suspicious documents, such as:
 - a. Documents provided for identification that appear to have been altered or forged.
 - b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
 - c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting identification.
 - d. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
 - iii. The presentation of suspicious personal identifying information, including:
 - a. Personal identifying information provided is inconsistent when compared against external information sources used by ClaimAid Self-Pay Solutions.
 - b. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by ClaimAid Self-Pay Solutions.
 - c. The Social Security number provided is the same as that submitted by other persons opening an account or other customers.

- d. 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 customers or persons opening accounts.
 - e. The customer or person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
 - f. Personal identifying information provided is not consistent with personal identifying information that is on file with ClaimAid Self-Pay Solutions.
 - g. When using security questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
 - iv. The unusual use of, or other suspicious activity related to, a covered account, such as:
 - a. Shortly following the notice of a change of address for a covered account, ClaimAid Self-Pay Solutions receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.
 - b. A new revolving credit account is used in a manner commonly associated with known fraud patterns.
 - c. A covered account is used in a manner that is not consistent with established patterns of activity on the account.
 - d. A covered account that has been inactive for a reasonable period of time is used.
 - e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
 - f. ClaimAid Self-Pay Solutions is notified the customer is not receiving paper account statements.
 - g. ClaimAid Self-Pay Solutions is notified of unauthorized transactions in connection with a customer's covered account.
 - h. ClaimAid Self-Pay Solutions receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
 - i. ClaimAid Self-Pay Solutions is notified by a customer, a victim of identity theft, law enforcement authorities, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
- B. The Program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:
 - i. The types of covered accounts offered or maintained.
 - ii. The methods provided to open covered accounts.
 - iii. The methods provided to access covered accounts.
 - iv. Its previous experience with identity theft.
- C. The Program shall incorporate relevant red flags from sources such as:
 - i. Incidents of identity theft previously experienced,
 - ii. Methods of identity theft that reflect changes in risk.
 - iii. Applicable supervisory guidance.

Detection of Red Flags

The Program shall 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.
- B. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

Responding to Red Flags

The Program shall provide for appropriate responses to detect red flags and to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses include but are not limited to:

- A. Monitor a covered account for evidence of identity theft.
- B. Obtaining a fraud affidavit or theft report from the consumer, which must be validated through local law enforcement or notary.
- C. Cease collection efforts.
- D. Close the existing covered account.
- E. Determine no response is warranted under the particular circumstances.

Periodic Updates to the Program

- A. At periodic intervals established in the Program, or as required, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current business environment.
- B. Red Flags may be revised, replaced, or eliminated. Defining new red flags may also be appropriate.
- C. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to ClaimAid Self-Pay Solutions and its customers.

Duties Regarding Address Discrepancies

- A. ClaimAid Self-Pay Solutions shall develop policies and procedures designed to enable ClaimAid Self-Pay Solutions to form a reasonable belief that a consumer report relates to the consumer for whom it was requested if ClaimAid Self-Pay Solutions receives a notice of address discrepancy from a consumer reporting agency indicating the address given by the consumer differs from the address obtained in the consumer report
- B. ClaimAid Self-Pay Solutions may reasonably confirm that an address is accurate by any of the following means:
 - i. Verification of the address with the consumer.
 - ii. Review of ClaimAid Self-Pay Solutions's records.
 - iii. Verification of the address through third party sources.
 - iv. Other reasonable means.
- C. If an accurate address is confirmed, ClaimAid Self-Pay Solutions shall furnish the consumer's address to the consumer reporting agency from which it received the notice of address discrepancy if:
 - i. ClaimAid Self-Pay Solutions establishes a continuing relationship with the consumer; and
 - ii. ClaimAid Self-Pay Solutions regularly and in the ordinary course of business, furnishes information to the consumer agency.

Physical Security of Personal Identifying Information Is Protected

- A. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
- B. All computer stations must be locked or logged off at the end of the workday.
- C. Access to offsite storage is limited to employees with a legitimate business need. Access keys/codes will only be given to those employees.
- D. Any sensitive information shipped using outside carriers or contractors will be encrypted.
- E. An employee of ClaimAid Self-Pay Solutions must escort visitors who must enter areas where sensitive files are kept.
- F. No visitor will be given any entry codes or allowed unescorted access to the office.

Security of Electronic Records

- A. General Network Security
 - i. Personally identifiable information that is sent to third parties over public networks will be encrypted.
 - ii. Personally identifiable information that is stored on the computer network or on disks or portable storage devices used by employees of ClaimAid Self-Pay Solutions will be encrypted.
 - iii. Any personally identifiable information sent externally must be encrypted and password protected and sent only to approved recipients. Additionally, a statement of confidentiality must be included which states the information is intended to whom it was originally address and any use by others is strictly prohibited.
 - iv. Anti-virus and anti-spyware programs will be run on individual computers and on servers on the network.
 - v. When credit card information is received or transmitted, Secure Sockets Layer (SSL) or another secure connection that protects the information in transit will be used.
- B. Password Management
 - i. Access to personally identifiable information will be controlled using “strong” passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be periodically changed.
 - ii. Passwords will not be shared or posted near workstations.
 - iii. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
 - iv. When installing new software, vendor-supplied default passwords will be immediately changed to a more secure strong password.
- C. Laptop Security
 - i. The use of laptops is restricted to those employees who need them to perform their jobs.
 - ii. Laptop users will only have access to personally identifying information, but will not store the information directly on the laptop.
 - iii. All laptops will be protected with strong passwords.
 - iv. Employees are never to leave a laptop visible in a car. If a laptop must be left in a vehicle, it must be locked in the trunk.
- D. Firewalls
 - i. A firewall must be used to protect computers from hackers while the computer is connected to the Internet.
 - ii. The computer network will have access controls that will be set to allow only trusted employees with a legitimate business need to access the network.
 - iii. Firewalls will be reviewed periodically.

Staff Training

- A. Staff training shall be conducted for all employees that may come into contact with account or personally identifiable information that may constitute a risk to ClaimAid Self-Pay Solutions or its customers.
- B. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the Program are made.