

Identity Theft Prevention Program

The purpose of the Identity Theft Prevention Program is to detect the warning signs – or “red flags” – of identity theft in our day-to-day operations. Preventing identity theft requires a 360° approach that goes beyond data security. As third-party administrator, we must be diligent in our efforts to look for signs of identity theft. If detected, we must take the necessary steps to mitigate its effect on the individual. This program provides our company with the information it needs to identify, detect and mitigate theft of its customers’ identifiable information for the purposes of stealing an individual’s identity.

Identified Relevant Red Flags for Identity Theft

- Notice from a customer, a victim of identity theft, a law enforcement agency or someone else that an account has been opened or used fraudulently.
- An enrollment form or application is received that looks like it has been altered, forged or torn up and reassembled.
- A Patriot Act review indicates the HSA enrollee does not match the information provided (address, social security number, employer).
- Frequent and repetitive use of debit card for ineligible items or at ineligible merchants.
- Mail or email sent to participant is returned repeatedly as undeliverable although transactions continue.
- Information received that participant is not receiving their account statements.
- Information received about unauthorized charges to the account.
- General inconsistencies with what we do know about the participant and account activity.
- A bogus address or a phone number that is invalid.
- A Social Security number that’s been used by someone else opening an account.
- A person omits required information on an application and doesn’t respond to notices that the application is incomplete.
- A person who cannot provide authenticating information beyond what’s generally available from a wallet or credit report – i.e. a person who cannot answer a challenge question.

Identify Theft Prevention Program

Detecting Red Flags

The following steps are followed to detect red flags associated with identity theft:

- Verifying missing or incomplete information on an enrollment form or application with an employer instead of with the employee directly.
- When meeting in person, verifying identity by obtaining a copy of a photo ID.
- Request changes to address, bank account information, or other personal information be provided in writing with signature required or through a secure login.
- Authenticate callers by asking them to verify their address, date of birth, employer and last four digits of their Social Security number.
- System programming that identifies duplicate Social Security numbers for employees within the system.

Responding to Red Flags

- Contact employer to verify employee information.
- Contact employee to determine if they have knowledge of purchases made using their debit card. Provide debit card paperwork to employee for reporting fraudulent transactions.
- Confirm with employee and employer the correct address for mail and email.
- If necessary close account and reopen a new account in the employee's name.

Identify Theft Prevention Program

Program Administrators:

Employee training for all employees is combined with HIPAA training and is conducted annually.

Service Providers affected by Red Flag Rule

Metavante – Benefits Debit Card Vendor

First Data (FD) – Benefits Debit Card Vendor

WiredCommute – Online transit pass/ parking pass vendor

The above service providers have verified to our company that they have an Identity Theft Prevention Program in place.

The Identify Theft Prevention Program was approved by the Board of Directors on (DATE).