
**DOUGLAS COUNTY ADMINISTRATIVE
POLICIES AND PROCEDURES**

NUMBER: 300.08
EFFECTIVE DATE: 04/16/09
REVISED:
AUTHORITY: BOC
COUNTY MANAGER: _____
PAGE 1 OF 5

SUBJECT: IDENTITY THEFT PREVENTION PROGRAM

I. PURPOSE: To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. This policy and protection program applies to employees, contractors, consultants, temporary employees and all other personnel affiliated with third parties.

II. POLICY:

A. DEFINITIONS:

1. **Identity theft** means fraud committed or attempted using the identifying information of another person without authority.
2. **Covered account** means:
 - a. 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, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts; and
 - b. 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 financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.
3. **Red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

III. PROCEDURE:

A. POLICY DEVELOPMENT:

In order to detect, prevent and mitigate identity theft, Douglas County will include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

B. ADMINISTRATION:

1. Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for Douglas County.
2. The Identity Theft Committee will consist of the County Clerk/Treasurer or designee, Assistant Clerk/Treasurer or designee, Information Systems Manager, Court Information Systems Manager, Airport Manager, Assistant County Manager, and a designee from Administrative Services Department, East Fork Fire and Paramedic Districts, District Attorney, and the Douglas County Sheriff's Department.
3. Staff shall be trained, as necessary, to effectively implement the Program;
4. The Program shall exercise appropriate and effective oversight of service provider arrangements.

C. IDENTIFICATION OF RED FLAGS:

1. The Program will include relevant red flags from the following categories as appropriate:
 - a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
 - b. The presentation of suspicious documents;
 - c. The presentation of suspicious personal identifying information;
 - d. The unusual use of, or other suspicious activity related to, a covered account;
 - e. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
2. The Program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:
 - a. The types of covered accounts offered or maintained;
 - b. The methods provided to open covered accounts;
 - c. The methods provided to access covered accounts;
 - d. Its previous experience with identity theft.
3. The Program will incorporate relevant red flags from sources such as:
 - a. Incidents of identity theft previously experienced;
 - b. Methods of identity theft that reflect changes in risk;
 - c. Applicable supervisory guidance.

D. DETECTION OF RED FLAGS:

The Program will address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account;
2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

E. RESPONSE:

The Program will provide for appropriate responses to detected red flags to prevent and mitigate identity theft. All responses will be documented and the response will be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft;
2. Contact the customer;

3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Reopen a covered account with a new account number;
5. Not open a new covered account;
6. Close an existing covered account;
7. Notify law enforcement; or
8. Determine no response is warranted under the particular circumstances.

F. STORING OF DOCUMENTS:

Each employee and contractor performing work for Douglas County will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, and other storage space containing documents with sensitive information will be locked when not in use.
2. Storage rooms containing documents with sensitive information and record retention areas will be located at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines and common shared work areas will be cleared of all documents containing sensitive information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
5. When documents containing sensitive information are discarded they will be placed inside a lock shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Locked shred bins are labeled “Confidential paper shredding and recycling.” Municipal records, however, may only be destroyed in accordance with the county’s records retention policy.

F. ELECTRONIC DISTRIBUTED DOCUMENTS:

Each employee and contractor performing work for Douglas County will comply with the following policies.

1. Internally, sensitive information may be transmitted using approved Douglas County email. All sensitive information must be encrypted when stored in an electronic format.
2. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the email:

“This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited.”

G. UPDATING THE PROGRAM:

The Program will be updated periodically to reflect changes in risk to customer or to the safety and soundness of the County from identity theft based on factors such as:

1. The experiences of the County with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in the types of accounts that the County offers or maintains;
5. Changes in the business arrangements of the County, including changes to service provider arrangements.

H. OVERSIGHT OF THE PROGRAM:

1. Oversight of the Program will include:
 - a. Assignment of specific responsibility for implementation of the Program;
 - b. Review of reports prepared by staff regarding compliance;
 - c. Approval of material changes to the Program as necessary to address changing risks of identity theft.
2. Reports will be prepared as follows:
 - a. Staff responsible for development, implementation and administration of the Program will report to the County Manager at least annually on compliance by the County with the Program.
 - b. The report will address material matters related to the Program and evaluate issues such as:
 - i. The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
 - ii. Service provider agreements;
 - iii. Significant incidents involving identity theft and management's response;
 - iv. Recommendations for material changes to the Program.

I. OVERSIGHT OF SERVICE PROVIDER AGREEMENTS:

The County will take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the County engages a service provider to perform an activity in connection with one or more covered accounts.

J. DUTIES REGARDING ADDRESS DISCREPANCIES:

1. The County will develop policies and procedures designed to enable the County to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the County receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.
2. The County will reasonably confirm that an address is accurate by any of the following means:
 - a. Verification of the address with the consumer;
 - b. Review of the utility's records;
 - c. Verification of the address through third-party sources; or
 - d. Other reasonable means.
3. If an accurate address is confirmed, the County will furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:
 - a. The County establishes a continuing relationship with the consumer; and
 - b. The County regularly and in the ordinary course business, furnishes information to the consumer reporting agency.

K. SPECIFIC PROGRAM ELEMENTS AND CONFIDENTIALITY:

For the effectiveness of Identify Theft Prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding Douglas County's specific practices relating to Identity Theft detection, prevention and mitigation. Under this Program, knowledge of such specific practices is to be limited to the Identity Theft Committee and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation and prevention practices are listed in this document.

IV. RESPONSIBILITY FOR REVIEW: The County Manager and County Treasurer will review this policy as needed or at least once every 5 years.

04/16/09