



Published on *County of Glenn* (<http://www.countyofglenn.net>)

[Home](#) > Identity Theft Policy

.19 Identity Theft Policy

- **.19.1 Purpose**

The purpose of the Identity Theft Policy is to comply with 16 CFR § 681.2 in order to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will prevent identity theft.

- **.19.2 Definitions**

For purposes of this Identity Theft Policy, the following definitions apply:

A. Covered account ? A consumer account that the County (creditor) offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account or mortgage loan, or a consumer account that allows payments subsequent to the provision of goods or services.

B. Red Flag - A pattern, practice, or specific activity that indicates the possible existence of identity theft.

- **.19.3 Identification of Red Flags**

All employees responsible for or involved in the process of opening a covered account, restoring a covered account or accepting payment for a covered account shall be on alert for red flags as indicators of possible identity theft and such red flags may include:

A. Alerts from consumer reporting agencies, fraud detection agencies or service providers.

B. Suspicious documents

C. Suspicious personal identifying information

D. Unusual use of, or suspicious activity related to, the covered account

Notice from the customer, law enforcement, victims, or other reliable sources regarding possible identity theft or phishing related to covered accounts.

.19.4 Detecting Red Flags

In order to facilitate detection of the Red Flags, employees should take the following steps to obtain and verify the identity of the person when there is a reasonably foreseeable risk to personally identifying information:

A. New Accounts

1. Require identifying information (e.g., full name, date of birth, address, government issued ID, insurance card, etc.)

B. Existing Accounts

1. Verify validity of requests for changes of billing address
2. Verify identification of customers before giving out any personal information

C. Credit Cards

1. Check a photo I.D.
2. Compare signature to the signature on the photo I.D.
3. If presented over the phone, request the validation code (3-digit code on the back of the card)

.19.5 Responding to Red Flags

Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the Supervisor, who in their discretion, shall determine whether such red flag or combination of red flags suggest a threat of identity theft.

A. The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

B. If, in the discretion of the Supervisor, it is determined that identity theft or attempted identity theft is likely or probable, appropriate actions must be taken immediately. Actions may include:

1. Denying the application or canceling the transaction;
2. Requesting additional identifying information from the customer/client/applicant;
3. Notifying and cooperating with appropriate law enforcement;
4. Determining the extent of liability of the County; and
5. Notifying the actual customer that fraud has been attempted.
6. Making the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's account:
 - a. Change any account numbers, passwords, security codes, or other security devices that permit access to an account; or
 - b. Close the account

7. Taking other reasonably appropriate action to prevent or mitigate identity theft.

•

.19.6 Oversight of Service Provider Arrangements

A. It is the responsibility of the County to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

B. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

C. Any specific requirements should be addressed in the appropriate contract arrangements.

-->

Source URL (modified on Apr 4 2016 - 3:52pm): <http://www.countyofglenn.net/identity-theft-policy>