

# Hanover County Identity Theft Prevention Program Standard Operating Procedure

**Applicability and Administration** – This Procedure implements the Identity Theft Prevention Program adopted by the Board of Supervisors and applies to all non-tax personal, family or household accounts, and all Departments that maintain such accounts. Please contact Finance if you are unsure of applicability to your accounts, or if you have any questions. This Procedure shall be interpreted and administered, and updated or amended as necessary by the County Administrator in compliance with the Red Flag Rules referred to below.

## **Purpose**

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 (administered by the Federal Trade Commission and known as the “Red Flag Rules”), the Hanover County Board of Supervisors (the County) has adopted the Identity Theft Prevention Program (ITPP or Program), as described in the County’s Revenue Policy and Regulations, to detect, prevent and mitigate identity theft in connection with the opening of a Covered Account, or an existing Covered Account and to provide for continued administration of the Program. This ITPP SOP incorporates detailed requirements contained in the Red Flag Rules in the Standard Operating Procedures of all Departments offering Covered Accounts, as necessary to fully comply with the Red Flag Rules and to fully implement the ITPP. This ITPP SOP shall be appended to the Standard Operating Procedures of each Department.

## **Definitions**

**For purposes of this policy, a “Covered Account”** means any non-tax account:

1. That a 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 utility accounts; and
2. Any other non-tax account that the 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.

**Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.

**Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or

any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

**Identifying information** is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, Social Security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol (IP) address, or routing code.

**Identity theft** means fraud committed or attempted using the identifying information of another person without authority.

**Red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

**Departments** mean any and all Departments that maintain Covered Accounts. Departments that currently maintain Covered Accounts include the Departments of Public Utilities, the Community Services Board, Fire/Emergency Medical Services, and Parks and Recreation. However, additional departments may be added to this ITPP SOP in the future, depending on periodic risk assessments of the risk of identity theft associated with County business operations and Covered Accounts. Departments which offer new types of non-tax accounts to customers should request a pre-determination from the Department of Finance as to whether the new accounts constitute "Covered Accounts" under this policy.

## **The Program**

As described in Hanover County's Revenue Policy and Revenue Regulations, the County has adopted this Identity Theft Prevention Program (ITPP) to detect, prevent and mitigate identity theft. The ITPP includes 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 incorporates, as appropriate, existing policies and procedures that control reasonably foreseeable risks of identity theft, including the County's Audit Policy, its IT Security and Use Policy and Procedures, and its HIPPA policy.

## Identification of Relevant Red Flags

In order to identify relevant Red Flags, the County considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts and its previous experience with Identify Theft. The County identifies the following red flags, in each of the listed categories:

- A. Notifications and Warnings From Credit Reporting Agencies (if used).
  - Report of fraud accompanying a credit report;
  - Notice or report from a credit agency of a credit freeze on a customer or applicant;
  - Notice or report from a credit agency of an active duty alert for an applicant; and
  - Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.
  
- B. Suspicious Documents
  - Identification document or card that appears to be forged, altered or inauthentic;
  - Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
  - Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
  - Application for service that appears to have been altered or forged.
  
- C. Suspicious Personal Identifying Information
  - Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
  - Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on the credit report);
  - Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
  - Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
  - Social Security number presented that is the same as one given by another customer;
  - An address or phone number presented that is the same as that of another person;
  - Failure to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and

- Inconsistency of a customer's identifying information with the information that is on file for the customer.

#### D. Suspicious Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (example: very high activity);
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice to the Department that a customer is not receiving mail sent by the Department;
- Notice to the Department that an account has unauthorized activity:
- Breach in the County's computer system security; or
- Unauthorized access to or use of customer account information.

#### E. Alerts from Others

- Notice to the locality from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

### **Detection of Red Flags**

#### **A. New Accounts**

In order to detect any of the Red Flags identified above associated with the opening of a new account, the Department's personnel will take one or more of the following steps, as documented in the Department's written procedures, to obtain and verify the identity of the person opening the account:

- Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
- Verify the customer's identity (for instance, review a driver's license or other identification card);
- Review documentation showing the existence of a business entity; and
- Independently contact the customer.
- Take other action(s) to verify identity as deemed appropriate by the Department Head and documented in the Department's written procedures.

## **B. Existing Accounts**

In order to detect any of the Red Flags identified above for an existing account, the Department's personnel will take one or more of the following steps as documented in the Department's written procedures, to monitor transactions with an account:

- Verify the identification of customers if they request information, whether in person, via telephone, via facsimile or via e-mail;
- Verify the validity of requests to change billing addresses; and
- Verify changes in banking information given for billing and payment purposes.
- Take other action(s) to monitor transactions as deemed appropriate by the Department Head and documented in the Department's written procedures.

**Written Departmental Procedures** - Actions adopted by each Department to verify the identity of persons opening new Covered Accounts and to monitor transactions of existing accounts may be specific to the size, complexity and nature of that Department's specific operations, and shall be documented by the Department in written procedures consistent with County policies. It is the responsibility of each employee to follow the written procedures, and of the Department Head to ensure appropriate periodic training and the consistent and effective performance of the written procedures specific to the Department.

### **Response to suspected identity theft**

In the event the Department's personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

- Continue to monitor an account for evidence of Identify Theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new number;
- Notify the Department Head for determination of the appropriate step(s) to take;
- Notify law enforcement;
- Take other action(s) as deemed appropriate by the Department Head; or
- Determine that no response is warranted under the particular circumstances.

In order to further prevent the likelihood of identity theft occurring with respect to customer accounts, the Department will take the following steps, when applicable, with respect to its internal operating procedures to protect customer identifying information:

- Take action to ascertain that its website is secure or provide clear notice that the website is not secure;
- Take action to completely and securely destroy paper documents and computer files containing customer information;
- Take action to ascertain that computers are password protected and that computer screens lock after a set period of time;
- Keep offices clear of unsecured papers containing customer information;
- Request personal information only upon approval by the Department Head of the request procedure, and only as necessary for business purposes;
- Take action to ascertain that computer virus protection is up to date; and
- Require and keep only the kinds of customer information that are necessary for the Department's purposes.
- Take additional actions(s) as deemed appropriate by the Department Head; and
- Contact the Internal Audit Department immediately to report any actual, suspected, or attempted identity theft.

### **Updating the ITPP SOP and Written Departmental Procedures**

The Finance Director, in consultation with the Departments, shall recommend amendments to this ITPP SOP as necessary to maintain compliance with federal or other requirements. Such amendments shall reflect changes in risks to customers or to the safety and soundness of the County from identity theft based on factors such as:

- The experiences of the Departments and County with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;
- Changes in the types of accounts that the Departments or County offers or maintains;
- Changes in the business arrangements of the Departments or County, including alliances, joint ventures and service provider arrangements.

**Written Departmental Procedures** - Each Department shall adopt departmental procedures as necessary to verify identity and otherwise comply with these SOPs and this Program. The procedures shall include details for staff guidance and shall be approved the Department Head.

### **Training**

The Departments shall train staff, as necessary, to effectively implement the ITPP.

### **Oversight of the Program**

1. Oversight of the ITPP shall include:

- a. Periodic review by the Departments of the ITPP SOP and recommendations for amendment to the County Administrator as necessary to address changing risks of identity theft.
- b. Preparation by the Departments and submission of periodic (at least annual) reports to the applicable Department Head and County Administrator regarding compliance with the ITPP. The report shall address material matters related to the ITPP and evaluate issues such as:
  - The effectiveness of the Program and the SOPs in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
  - Compliance of service provider agreements;
  - Significant incidents involving identity theft and management's response; and
  - Recommendations for material changes to the ITPP.

### **Oversight of Service Provider Arrangements**

In the event the Department engages a service provider to perform an activity in connection with one or more accounts, its Fiscal Contact or Business Manager will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

- Require, by contract, that service providers have effectively operating ITPP policies and procedures in place; and provide evidence of such to the County, or
- Require, by contract, that service providers perform their work in substantial compliance with the County's ITPP and report any Red Flags to the Hanover Department Head, who shall report them to the Hanover Director of Internal Audit.

### **Duties Regarding Address Discrepancies (if credit reports are used)**

The Department shall develop a standard operating procedure designed to enable it to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the Department receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

The Department may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the consumer;

2. Review of the Department's records;
3. Verification of the address through third-party sources; or
4. Other reasonable means.

If an accurate address is confirmed, the Department shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. The Department establishes a continuing relationship with the consumer; and
2. The Department, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.