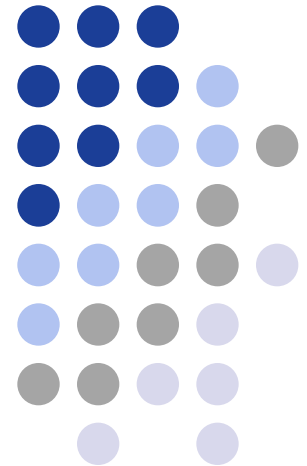
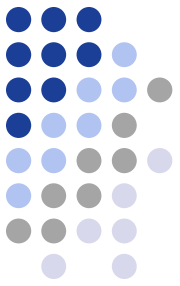


Corporate Identity Theft Prevention Program

The “Red Flag” Rules
Effective December 31, 2010

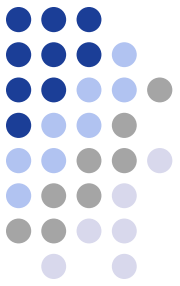


TISC has developed an Identity Theft Prevention Program



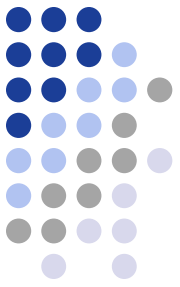
- In compliance with new FTC rules, this program applies to all affiliated companies.
- The program is designed to detect, prevent and mitigate identity theft in connection with the opening of, or current use of a covered account with our company.

The Program is designed to:



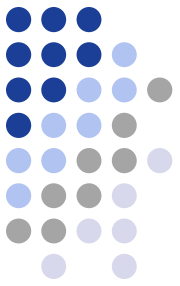
- Identify “Red Flags” for the covered accounts
- Detect “Red Flags” that been incorporated in the program
- Respond to any “Red Flags” that are detected to prevent and mitigate ID theft
- Ensure the Program is updated periodically

Definition of a Covered Account

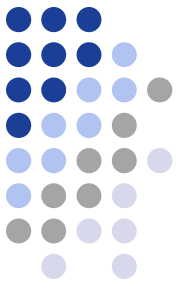


- Any account that is offered or maintained by a communications company and its affiliates that is designed to allow for multiple payments or transactions. Refers specifically to telecommunications services to Customers for which there is foreseeable risk of ID Theft.

Red Flags and CPNI



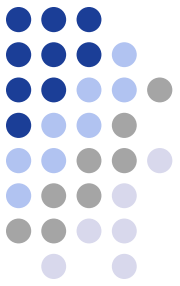
- The rules have been designed to compliment current CPNI rules
 - Requires verified passwords to access on-line private information regarding details of personal covered accounts
 - Requires use of a valid government issued Photo-ID before obtaining in-person information to data.



Identifying Red Flags

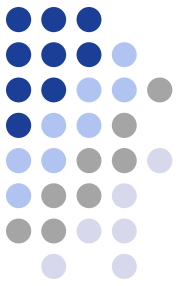
- Based on Risk Factors:
 - **Type of Account:** prepaid vs. in arrears
 - **Methods of payment:** in person, online or over the phone
 - **Methods to Open Accounts-** in person, online or over the phone
 - **Methods of Access to Account-** Accounts-in person, online or over the phone
 - Previous experience with ID Theft

Sources of Red Flags



- Sources include:
 - Previous experience with Identity Theft
 - Changes in identity theft activity and methodology
 - Supervisory guidance

Categories of Red Flags



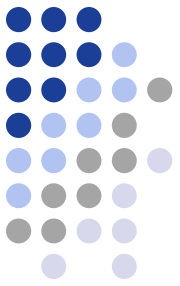
- Examples as contained in FTC Rules:
 - Alerts from consumer reporting agencies or service providers
 - Suspicious documents
 - Suspicious ID or address changes
 - Unusual account activities
 - Notice from customers, law enforcement agencies or other reliable sources

Detecting Red Flags



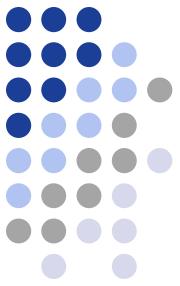
- The program procedures address the detection of Red Flags in connection with opening accounts or existing accounts by:
 - Obtaining ID information about, and verifying the ID of a person opening or seeking information about an account.
 - Authenticating customers, monitoring transactions and verifying the validity of change of address requests in the case of an existing account.

Preventing or Mitigating ID Theft



- If the company detects a Red Flag it may take any or all of the following steps:
 - Monitor the covered account for evidence of ID Theft
 - Contact the customer using CPNI information
 - Change the passwords that permit access to data
 - Reopen the account with a new account number
 - Not open a new account
 - Close an existing covered account
 - Not attempt to collect on a covered account or not sell an account to a debt collector
 - Notify law enforcement
 - Determine no response is necessary

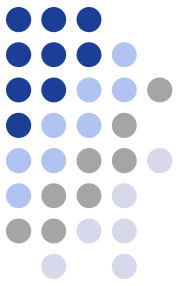
Minimize the Use of Personal Identifying Information



- To include:
 - Social Security numbers
 - Drivers license numbers
 - Other forms of personal identifying information

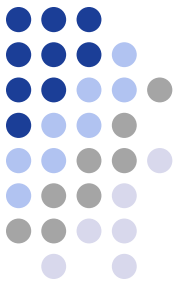
When this type of information is gathered, it is stored in a locked or secure area where access is limited to employees with authorization to view such information (need to know basis).

Credit Cards



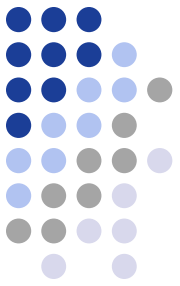
- We accept credit cards for payment, but the information is stored in a locked area.
- Electronic payments are accepted via the internet and are secured using licensed internet security software.

Designated Employee for Red Flag Activities



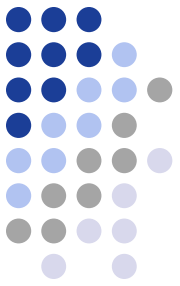
- All Red Flag activities are to be reported to the Human Resource Manager for oversight, development, implementation and administration of the Red Flag program.
- The Human Resource manager shall have the responsibility to determine what course of action should be taken to protect the customer from potential ID theft.
- Other management personnel may be designated by the Human Resource Manager to assist with the program as needed.

Compilation of Red Flag Data



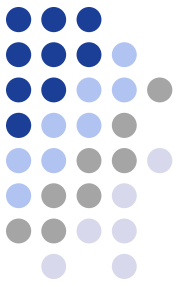
- The Human Resource Manager shall compile all data surrounding the Red Flag program and will report this data to the Board of Directors annually.
- This report will be done at the same time as the CPNI data report while using the established CPNI procedures

Training of Employees



- At least annually all employees shall be updated on Red Flag procedures.
- Records of trainings will be maintained for three years following the date of an employees termination from the company.

Annual Review by the Board of Directors



The board of Directors shall annually review the program and make changes as needed. All changes to the program must be approved by the Board and be reflected in the board minutes.