Attachment A

King County
King County **Department Policies and Procedures**

General Department
Policies & Procedures

Title Policy:	Document Code No.
Identity Theft Prevention Program	DP-FIN-062010
Department/Issuing Agency: Department of Natural Resources and Parks	Effective Date: June 1, 2010

Approved
Bob Burns

1.0 SUBJECT TITLE: Identity Theft Prevention Program

1.1 Effective Date: June 1, 2010

1.2 Type of Action: New

1.3 Key Words: Fraud, Identity Theft, Red Flag, Service Provider.

2.0 PURPOSE:

To establish a policy within the Department of Natural Resources and Parks (DNRP) outlining protocols, standards, schedule, responsibilities and associated actions aimed meet the requirements set forth in the Federal Trade Commission's (FTC) Red Flags Rules mandated by 16 CFR § 681.1.

3.0 ORGANIZATIONS AFFECTED: Applicable to the Department of Natural Resources and Parks (DNRP).

4.0 REFERENCES:

4.1 Fair and Accurate Credit Transactions Act of 2003 (FACTA)

4.2 16 CFR § 681.1- Federal Trade Commission Identity Theft Rules

4.3 KC DNRP Wastewater Treatment Division Identity Theft Prevention Program (Appendix)

5.0 DEFINITIONS:

5.1 "Account" means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.

5.2 "Covered Account" means:

a) any account DNRP business units offer or maintain primarily for personal, family or household purposes, that involves multiple payments or transactions (currently only the Capacity Charge Program associated with our Wastewater Treatment Division utility meets this definition); and

b) any other account the Department offers or maintains for which there is a foreseeably reasonable risk to customers or to the safety and soundness of the Department from Identity Theft.

5.3 "Fraud" means an intentional deception made for personal gain or to damage another individual.

5.4 "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

5.5 "Mitigation" means activities designed to lessen the severity or intensity of damage created by identity theft.

5.6 "Red Flags" means potential patterns, practices, or specific activities indicating the possibility of identity theft.

6.0 POLICIES:

6.1 DNRP will maintain and administer an Identity Theft Prevention Program in order to detect, prevent, and mitigate financial identity theft.

6.2 The Chief Financial Officer (CFO) is the chief official for this policy and is responsible for the administration and maintenance of the policy.

6.3 Administration of this policy shall include an annual review of DNRP's business units to determine whether any additional units have accounts covered by Section 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. At the outset of this program's development we found only one business unit that has a covered account: the Capacity Charge Program in our Wastewater Treatment Division (see Appendix A: Identify Theft Prevention Program for Wastewater Treatment Division).

6.4 Maintenance of this policy shall include annual review of the policy language and procedures to ensure that it is kept current and relevant.

7.0 PROCEDURES

Action By: Chief Financial Officer

Action:

7.1 Annually, the CFO shall initiate a review process to identify any additional DNRP business units that may have covered accounts.

Action By: Division Finance Managers

Action:

7.2 Where covered accounts are identified within their divisions, Division Finance Managers shall develop division level compliance procedures consistent with this policy and its purpose. Division-level procedures will be incorporated as appendices to this policy as part of the annual policy review process.

7.3 Either assume or designate responsibility to serve as the Program Administrator for the Division-level Identity Theft Prevention Program.

Action By: Chief Financial Officer

Action:

7.4 Where indicated by the development of new or revised division level procedure documents (which are appended to this policy document), the CFO shall make necessary updates to this Department Policy to incorporate appropriate language revision and the addition of or revision to appendices.

8.0 RESPONSIBILITIES:

8.1 CFO is responsible for initiating and conducting an annual review of accounts to determine whether there are additional covered accounts.

8.2 Division Financial Officer is responsible for developing division level compliance procedures for covered accounts and for serving as or assigning a Program Administrator to implement the compliance procedures for the division.

8.3 Program Administrator coordinates and has oversight for the implementation of division-level compliance procedures, which might also be known as a division-level Identity Theft Prevention Program.

9.0 APPENDICES:

9.1 KC DNRP Wastewater Treatment Division Identity Theft Prevention Program

Appendix A

King County Department of Natural Resources and Parks
Wastewater Treatment Division

Identity Theft Prevention Program
Effective June 1, 2010

I. PROGRAM ADOPTION

The county's Wastewater Treatment Division ("Division"), Department of Natural Resources and Parks, staff developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of the Division's operations and account systems, and as well as the nature and scope of its activities, this Program was developed and became an administrative policy of the Division with oversight by the Department's Chief Financial Officer ("Program Administrator").

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling Requirements of the Red Flags Rule

Under the Rule, every financial institution and creditor is required to establish a Program tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts 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 or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule Definitions Used in This Program

For the purposes of this Program, the following definitions apply:

1. Account. "Account" means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.
2. Covered Account. A "covered account" means:
   a. Any account the utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
   b. Any other account the Division offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Division from Identify Theft.

3. Creditor. "Creditor" means a person or entity that arranges for the extension, renewal or continuation of credit, including the Division's Capacity Charge Program.

4. Customer. A "customer" means a person or business entity that has a covered account with the Division.

5. Financial Institution. "Financial institution" means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a customer.

6. Identifying Information. "Identifying information" means 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 or unique electronic identification number.

7. Identity Theft. "Identity theft" means fraud committed using the identifying information of another person.

8. Red Flag. A "red flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

9. Service Provider. "Service provider" means a person or business entity that provides a service directly to the Division relating to or in connection with a covered account.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the Division shall review and consider the types of covered accounts that it offers and maintains, the methods it provides to open covered accounts, the methods it provides to access its covered accounts, and its previous experiences with Identity Theft. The Division identifies the following potential Red Flags, in each of the listed categories which might affect the Division's covered accounts:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

Because the Division does not obtain a customer's credit history before opening an account, the Division does not receive notifications or warnings from credit reporting agencies and, therefore, has not identified any red flags in this category.

B. Suspicious Documents

Red Flag

1. Documents with information that is not consistent with existing customer information.

C. Suspicious Personal Identifying Information

Red Flags

1. Incomplete identifying information on a residential or non-residential sewer use certification form submitted by the local sewer agency; and
2. Identifying information on a residential or non-residential sewer use certification form submitted by a property owner rather than the local sewer agency.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Any attempt to use a credit card to pay an account when the name on the card is different from the customer listed on the account; and
2. Breach in the Division's computer system security.

E. Alerts from Others

Red Flag

Because the Division does not obtain a customer's credit history before opening an account for a customer, the Division does not receive notifications or warnings from credit reporting agencies and, therefore, has not identified any red flags in this category.

IV. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, Division personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect Red Flags

1. Only open a new account if the residential or non-residential sewer use certification form is complete and was submitted to the Division by a local sewer agency that is in compliance with the Red Flags Rule; and
2. Verify billing information for a business entity.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, Division personnel will take the following steps to monitor transactions with an account:

Detect Red Flags

1. Require requests to change billing addresses to be in writing or verify a change of address using parcel viewer; and
2. Require certain identifying information such as name or residential or business address, as well as the security code on the credit card, before accepting a credit card payment.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Division 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:

A. Prevent and Mitigate Identity Theft

1. Contact the customer with the covered account;
2. Not open a new covered account;
3. Notify the Program Administrator for determination of the appropriate step(s) to take;
4. Notify law enforcement; or
5. Determine that no response is warranted under the particular circumstances.

B. Protect Customer Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Division accounts, the Division shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Secure the Division website but provide clear notice that the website is not secure;
2. Make office computers password protected and provide that computer screens lock after a set period of time;
3. Require personnel to enter all credit card payment information directly into the computer without writing down the information;
4. Personnel accepting credit card information in order to process a payment shall be required to sign an Acknowledgement of Information Security Responsibilities and Confidentiality.
5. Maintain computer virus protection up to date; and
6. Require and keep only the kinds of customer information that are necessary for Division purposes.

VI. PROGRAM UPDATES

The Program will be periodically reviewed and updated to reflect changes in risks to customers and to the safety and soundness of the Division from Identity Theft. The Program Administrator shall at least annually consider the Department's experiences with Identity Theft, changes in Identity methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Department maintains and changes in the Department's business arrangements with other entities and service providers. After considering these factors, the Program Administrator shall determine whether changes to the Program, including the listing of Red Flags, are warranted.

VIII. PROGRAM ADMINISTRATION.

A. Oversight

The Program Administrator shall be responsible for the Program administration, reviewing any staff reports regarding the detection of Red Flags, the steps for preventing and mitigating taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

Division staff responsible for implementing the Program shall be trained either by or under the direction of the Division Finance Manager in the detection of Red Flags, and responsive steps to be taken when a Red Flag is detected.

C. Service Provider Arrangements

In the event the Division engages a service provider to perform an activity in connection with one or more covered accounts, the Division shall take the following steps to require that the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to Division covered accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Program Administrator relative to the Program and agree to report promptly to the Division in writing if the service provider in connection with a Division covered account detects an incident of actual or attempted identity theft or is unable to resolve one or more Red Flags that the service provider detects in connection with a covered account.

D. Customer Identifying Information and Public Disclosure

The identifying information of Division customers with covered accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law.