COUNTY DEPARTMENT AGENDA REQUEST

Department:	Finance	Presenter(s):	Tony Parrott
Meeting Date:	Thursday, April 23, 2009	Type of Request:	New Business

Wording for the Agenda:

Consideration of staff's recommendation that the County adopt a policy to be known as the Fayette County Identity Theft Program designed for the detection, prevention, and mitigation of identity theft pertaining to customers' accounts administered by the Fayette County Water System.

Background/History/Details:

The federal Fair and Accurate Credit Transactions Act of 2003 (Public Law 108-159) designates certain federal agencies to (A) establish guidelines for use by credit-lending entities regarding identification of "red flags" that could indicate identity theft, and (B) prescribe regulations requiring each of the covered entities to establish reasonable policies and procedures for implementing the guidelines established to identify risks to account holders. The federal agencies charged with this task published the resulting regulations in section 16 CFR 681.2 of the Code of Federal Regulations. The regulations include public utilities such as water systems in the definition of "creditor," so the Water System is required to comply with the stipulations of the regulations.

Regulations at 16 CFR 681.2 provide that each creditor must "develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account." It says that the creditor must "obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors." Once the initial approval of given by the Board, updates or other changes can be made by a appointed "senior-level manager" who is appointed to oversee the program. The Federal Trade Commission and other involved federal agencies required that the program be in place by May 1, 2009.

What action are you seeking from the Board of Commissioners?

To obtain approval of the policies and procedures developed to constitute the county's Identity Theft Prevention Program as required by federal Public Law 108-159.

If this item requires funding, please describe:

Not Applicable.

Has this issue come before the Commissioners in the past?	No	If so, when?	
Do you need audio-visual for the presentation?	No	Back-up Material Submitted?	Yes

STAFF USE ONLY

Approved by Finance	Yes	Reviewed by Legal	Yes
Approved by Purchasing	Yes	Approved by County Clerk	Yes
Administrator's Approval	Yes		

Staff Notes:

Fayette County GEORGIA

Where Quality Is A Lifestyle

To: Mary S. Holland

From: Ted L. Burgess

Date: April 7, 2009

Subject: Identity Theft Prevention Program

The federal Fair and Accurate Credit Transactions Act (FACT Act) of 2003, which is designated as Public Law 108-159, was signed into law by former President Bush on December 4, 2003. It required the Federal Trade Commission, the National Credit Union Administration, and the federal banking agencies to jointly establish regulations for the identification of patterns, practices, or specific forms of activity (called "red flags") that indicate the possibility of identity theft. The federal agencies developed guidelines to implement the program, and published them in section 16 CFR 681 of the Code of Federal Regulations.

The regulations require that any public or private entity must develop and implement an Identity Theft Prevention Program if they provide customers with an:

- *Account* – defined as a continuing relationship established so that a person, family, household, or business can obtain a product or service, and then be billed afterward. Since the service is provided before the customer is billed, this is said to "extend credit".
- *Covered account* – defined as:
    - An account (as defined above) that involves multiple payments or transactions, such as a credit card account, mortgage loan, cell phone account, checking or savings account, or utility account; and
    - Any other account (as defined above) for which there is a reasonably foreseeable risk to customers or the public or private entity from identity theft.

The county's Water System falls within the regulations, since it does establish accounts, provide a service, then bill customers afterward at the end of the month. Other county services, such as business licenses or ad valorem taxes, do not fall within the definition because they do not extend credit while providing a service.

In this county, a person can open a water account in person or over the telephone by contacting the Water System. Customers can pay bills in person or through the mail. Beginning April 6, 2009 customers can pay bills on-line by credit card, debit card, or electronic check. The on-line payments will be processed by a third-party service provider. The process will include the following steps:

- A customer goes on-line to the Water System page on the county web site. A link will put them through to the web site of Paymentus.com.
- Paymentus.com is the third-party payment service. They accept the debit card, credit card, or electronic check payment. They create an electronic file with customer information, which is uploaded to the Water System. They forward transaction information electronically to Chase Paymentech.
- Chase Paymentech verifies that the credit card or other transaction instrument is legitimate, that the customer's account is in good standing, and other related information. After processing the information, Chase Paymentech sends it electronically to Wachovia Bank for settlement.

An important component of the Identity Theft Prevention Program regards these third-party service providers. The regulations state that the county "should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, {the county} could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the {county}, or to take appropriate steps to prevent or mitigate identity theft."

Federal regulations require that the Board of Commissioners must approve the initial written policy. Thereafter, the program's policies and procedures can be updated at the discretion of "the Board, a committee, or senior management." The regulations also allow for a member of senior management to be appointed to provide oversight, development, implementation, and administration of the program. The policies and procedures include a provision for the Water System Director to be the appointed member of senior management.

April 7, 2009

Fayette County, Georgia
Identity Theft Prevention Program

PURPOSE

Public Law 108-159, the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), was signed into law by the President on December 4, 2003. The FACT Act directed the Federal Trade Commission, the federal banking agencies, and the National Credit Union Administration to jointly establish regulations for the identification of patterns, practices, or specific forms of activity (called "red flags") that indicate the possibility of identity theft. The resulting guidelines were published in section 16 CFR 681 of the Code of Federal Regulations. The regulations require local governments to establish identity theft programs for "covered accounts." Water services or other utilities are covered accounts. These policy and procedures establish the Identity Theft Program for the county's Water Services.

POLICY

Program Objectives: Fayette County's Identity Theft Prevention Program is established to enhance protection of financial and other personal information of customers of the Water System. Procedures are designed to (1) *identify* red flag activities that indicate possible identity theft; (2) *detect* red flags that have been identified, determined relevant, and incorporated into the Program; (3) *respond* appropriately to red flags that are detected, in order to prevent or mitigate identity theft; and (4) ensure the Program is updated periodically, to reflect changes in risks to Water System customers, or to the safety and soundness of the county, from identity theft.

Program Oversight and Administration: The Water System Director is designated as the senior-level manager to provide oversight, development, implementation and administration of the Program. Duties of the Director include, but are not limited to, the following:

- The types of covered accounts maintained;
- Assign specific responsibilities for Program implementation;
- Approve or initiating material changes to the Program as necessary to address changing identity theft risks.
- Periodically provide reports to the County Administrator and Board of Commissioners regarding compliance with federal requirements for the Program.
- Provide for requirements that relevant service providers have adequate safeguards in place to detect and respond to red flags.

- Provide for periodic staff training, as necessary, to assure the effectiveness of the Program.

PROCEDURES

A. **Identification of red flag activities**: The Water System has reviewed processes and operating procedures to identify activities that should be considered red flags. This was accomplished using guidance provided by the FACT Act and federal regulations found in 16 CFR 681.2, and considering:
   - methods used to open water service accounts,
   - methods used to access accounts, and
   - previous experience regarding identity theft.

   Following is a list of activities that are considered red flags in prevention and intervention of identity theft:

   Suspicious Documents

   1. Documents provided for identification appear to have been altered or forged.
   2. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
   3. Other information on the identification is not consistent with readily accessible information that is on file with the Water System, such as an existing signature or a recent check.
   4. A service application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

   Suspicious Personal Identifying Information

   5. Personal identifying information provided is inconsistent when compared against external information readily available to the Water System.
   6. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
   7. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Water System. For example, the address or phone number on an application is the same as that provided on a fraudulent document.
   8. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources. For example, the address on an application is

fictitious, a mail drop, or a prison, or the phone number is invalid or associated with a pager or answering service.

9. The address or telephone number provided is the same as, or similar to, the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
10. The person opening the covered account, or the customer, fails to provide all required personal identifying information on an application, or in response to notification that the application is incomplete.
11. Personal identifying information provided is not consistent with personal identifying information that is on file with the Water System.

Suspicious Activity Related to the Covered Account

12. Change of address is requested for an account, followed by a request to change the account holder's name.
13. Mail sent to the account holder is repeatedly returned as undeliverable.
14. Notice is given to the Water System that a customer is not receiving mail sent by the System.
15. A breach is made in the Water System's computer system security.
16. There is unauthorized access to, or use of, customer account information.

Notice from Customers, Victims of identity Theft, Law Enforcement Authorities, or Others Persons Regarding Possible Identity Theft in Connection With Covered Accounts

17. The Water System is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

B. **Detection of Activities that have been Identified as Red Flags**:

New Accounts: In order to detect any of the above red flags that pertain to opening a new account, Water System personnel will take the following steps to obtain and verify the identity of the person opening the account:

- For a residential account, require adequate identifying information such as the new customer's name and residential address.
- For a business account, require adequate identifying information, such as the applicant's name, business address.
- Independently contact the customer.

Existing Accounts: In order to detect any of the above red flags for an existing account, the Water System's personnel will take the following steps to monitor account transactions:

- Verify the identification of customers if they request information, whether in person, via telephone, via facsimile, or via e-mail.

C. **Response to Red Flags**: In the event that a Water System employee becomes aware of red flag(s), the employee shall immediately report the red flags to his or her supervisor. If the supervisor, in his or her discretion, determines that further action is needed, a Water System employee shall perform one or more of the following responses, as determined appropriate:

1. Contact the customer.
2. Take the following steps if, after contacting the customer, it is apparent that someone else has accessed the account:
   a. Change any account numbers, passwords, security codes, or other access to the account; or
   b. Close the account.

3. Cease attempts to collect additional charges from the customer. Decline to sell the customer's account to a debt collector in the event that unauthorized access has caused additional charges to accrue.
4. If the customer's account has been sold to a debt collector, notify the debt collector as soon as reasonably possible of a discovery of actual or possible identity theft.
5. Notify law enforcement.
6. Take other appropriate action to prevent or mitigate identity theft.

D. **Updating the Program**: The Water System will update the Identity Theft Prevention Program periodically, in order to reflect changes in risks to customers, or changes to the safety and soundness of the billing and service system, as relates to identity theft. The frequency of updates will be based on factors such as:

- Experience of the Water System with actual or attempted identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts used; or
- Changes in the business arrangements of the Water System with third-party service providers or others.

E. **Third-Party Service Providers**: The Water System provides a number of services to customers through third-party service providers. These include payment processors, banks, and others. The Water System will assure, through contractual agreement, that any service provider receiving or processing customers' personal information has an identity theft prevention program in place. The service provider shall have policies and procedures to detect relevant red flags that may arise in the performance of services, and either report the red flags to the Water System or take appropriate steps to prevent or mitigate identity theft.

F. **Reports**: The Director of the Water System shall report to the Board of Commissioners as needed, but at least annually, on material matters and compliance related to the Identity Theft Prevention Program. The report shall include, as appropriate, such issues as the effectiveness of the Water System in addressing the risk of identity theft in opening new accounts or existing accounts; service provider arrangements; significant incidents involving identity theft and management's response; and any material changes to the program.