LEGISLATIVE, FINANCE, AND ADMINISTRATION COMMITTEE

A G E N D A

March 23, 2009 - 6:00 P.M. - Council Chambers - City Hall - City of Dover

Public comments are welcomed on any item and will be permitted at appropriate times. When possible, please notify the City Clerk (736-7008 or e-mail at Tmcdowell@dover.de.us) should you wish to be recognized.

AGENDA ADDITIONS/DELETIONS

1. Review and Recommendation - Filling Critical Positions

2. Identity Theft Prevention Policy

3. Adjournment by 7:00 P.M.

/tm
S:\ClerksOffice\Agendas&Minutes\Committee-Agendas\2009\03-23-2009 LF&A.wpd

THE AGENDA ITEMS AS LISTED MAY NOT BE CONSIDERED IN SEQUENCE. THIS AGENDA IS SUBJECT TO CHANGE TO INCLUDE THE ADDITION OR THE DELETION OF ITEMS, INCLUDING EXECUTIVE SESSIONS.

ACTION FORM

PROCEEDING: Legislative, Finance and Administration	**AGENDA ITEM NO**:
DEPARTMENT OF ORIGIN: City Manager's Office	**DATE SUBMITTED**: 3/23/2009
PREPARED BY: Teresa Tieman, Senior City Administrator	
SUBJECT: Identity Theft Prevention Policy	
REFERENCE: Fair and Accurate Credit Transaction Act of 2003 (FACT Act)	
RELATED PROJECT: N/A	
APPROVALS: Committee/Council	
EXHIBITS: Presentation, Policy and Exhibits	
EXPENDITURE REQUIRED: N/A **FUNDING SOURCE (Dept./Page in CIP & Budget)**: N/A	**AMOUNT BUDGETED**: N/A
TIME TIMETABLE: N/A	
RECOMMENDED ACTION: Approval of the Identity Theft Prevention Policy	

BACKGROUND AND ANALYSIS: The FACT Act (2003) was passed to set standards for guarding customer information. It took effect January 1, 2008; however, entities covered by the rule have until May 1, 2009, to implement programs to comply with the rule. The rule requires creditors (which includes utilities or any entity that would process payments and establish ongoing accounts) to establish identity theft prevention programs for covered accounts. On November 1, 2007, the red flags (patterns or particular specific activities that indicate possible risk of identity theft) were added to hold businesses liable for the prevention, detection and mitigation of identity theft.

The FACT Act requires The City to develop a privacy policy; identify red flags; perform a needs assessment; document choices for mitigation; use best practices for record disposal; document employee training; document employee screening; form a privacy committee; document procedures for handling a breach in security; document procedures for handling address discrepancies; document procedures for handling a customer's request for information; document internal and external IT security procedures; document complaints; perform yearly assessments; and compile annual reports for internal purposes. As we proceed through these tasks the current policy may need to be revised.

The Federal Trade commission enforces the FACT Act. Punitive fines are expected to represent the degree of negligence and total loss, therefore, the City must demonstrate "reasonable security" of our customer's information.

Beginning in October 2008 thru February 2009, members of the Privacy Committee met and reviewed the City's current policies and procedures. The committee also identified red flags, performed needs assessments and review procedures for handling a breach in the security of customer information. The previous policy submitted in October was also reviewed for the City's purposes.

CITY OF DOVER
IDENTITY THEFT PREVENTION POLICY

Subject: Identity Theft Prevention Program for the City of Dover

Purpose: To create and implement an Identity Theft Prevention Program for the City of Dover that will identify, detect, prevent and mitigate, and update Red Flags that signal the possibility of identity theft in connection with the opening of a covered account or any existing covered account and payment of services.

Effective Date: May 1, 2009

STATEMENT OF POLICY

The Fair and Accurate Credit transaction Act (the FACT Act), which amends the Fair Credit Reporting Act (FCRA) established numerous requirements that provide protection for the victims of identity theft, provide more information to consumers about credit reports and credit scoring, limits sharing of information with affiliates, and protects consumer medical and other information.

POLICY

It is policy of the City of Dover to:

- Respond to fraud and activity duty alerts.
- Properly dispose of consumer report information.
- Provide information to victims of identity theft.
- Properly handle notice of identity theft.
- Respond to any notification received from identity theft, to prevent refurbishing blocked information.
- Truncate all but the last 4 digits of a debit or credit card and social security number.
- Comply with the rules regarding sharing information with affiliates.
- Provide an oral, written, or electronic notice to those who receive less favorable terms.
- Provide the required notice and credit scores, upon request.
- Provide notice regarding negative information.
- Take appropriate action when the utility receives a notice of discrepancy in the consumer's address.
- Comply with red flag guidelines.
- Protect medical information in the utility system.

The Privacy Officer, with assistance from the Privacy Committee members, is responsible for developing appropriate written procedures and internal controls to assure compliance with the act.

The senior officer of each department is responsible for implementing and complying with these procedures and internal controls.

DEFINITIONS

Covered Account

For purposes of this Policy, the term means an account that the City of Dover offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions **and** any other account that the City of Dover offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of the City of Dover from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Identity Theft

For purposes of this Policy, the term means a fraud committed or attempted by using personal identifying information (name, social security number, etc.) of another person without authority. This fraudulent activity may include opening deposit accounts with counterfeit checks, establishing credit card accounts, establishing lines of credit, or gaining access to the victim's accounts with the intent of depleting balances.

Privacy Officer

The person appointed the responsibility to oversee the procedures of this policy including periodic assessments, employee training, and annual reporting.

Red Flag

For purposes of this Policy, the term means a pattern, practice, or specific activity that indicates the possible existence, intent, or risk of identity theft. The section titled "Identification of Relevant Red Flags" provides a specific description of which Red Flags are applicable to this policy.

PRIVACY COMMITTEE

On ***October 15, 2008*** the Privacy Committee was formed under the leadership of ***Teresa Tieman, Senior City Administrator***. Each representative qualifies under a "need to know" guideline. For security, only employees who have been carefully screened and/or have a successful tenure with the utility will qualify.

Representation from key areas included:

Name	Department	Responsibilities/ Areas of Expertise
Teresa Tieman	City Manager's Office	**Privacy Officer -** Will coordinate activities of the committee/ develop and evaluation of program. Reports to: City Manager
Teresa Tieman	City Manager's Office	Supply resources to establish proactive identity theft program.
Peggy Teal	Accounting	Payroll, Specialist in the flow of funds.
Andy Siegel/ Mark Callan	IT	Data and Network Security, Specialist in SCADA/network administration.
Rhonda Walker	Human Resources	Personnel Information. Identity Theft Training.
Sgt. Tim Stump	Police	Fraud Investigator
Kathy Divver	Customer Service	Day to day processes in opening new accounts and monitoring activity on existing accounts. Billing, Collections
Carolyn Courtney	Recreation	Day to day processes in opening new accounts and monitoring activity on existing accounts.
Maretta Purnell/Scott Koenig	Public Services, Permitting/Licensing	Day to day processes in opening new accounts and monitoring activity on existing accounts.
Lisa Gardner	Public Utilities	Day to day processes in opening new accounts and monitoring activity on existing accounts
Traci McDowell/Amber Clendaniel	City Clerk	Records Retention

IDENTIFICATION OF RELEVANT RED FLAGS

After careful examination of our accounts, including the methods by which we open and access accounts, and our past experience with identity theft, the following events/occurrences reasonably indicate the potential for identity theft and should be considered "Red Flags" for purposes of this policy:

A. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detections services. For the purposes of this policy the City of Dover will be utilizing TransUnion as our service provider to identify the "Red Flags" listed below:

1. A fraud or active duty alert is included with a credit report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a credit report.

3. A consumer reporting agency provides a notice of address discrepancy.

4. A credit report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. The presentation of suspicious documents, such as, but not limited to:

1. Documents provided for identification appear to have been altered or forged.

2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

4. Other information on the identification is not consistent with readily accessible information that is on file. For example, the signatures do not match the signature card on file or a recent check.

5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. The presentation of suspicious personal identifying information, such as a suspicious address changes:

1. Personal identifying information provided is inconsistent when compared against external information sources used by the City of Dover. For example:

a. The address does not match any address in the credit report; or
b. The Social Security Number (SSN) has not been issued, or
c. The Social Security Number is listed on the Social Security Administration's Death Master File.

2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the date of birth on a driver's license and on other forms of identification provided.

3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City of Dover. For example:

   a. The address on an application is the same as the address provided on a fraudulent application; or
   b. The phone number on an application is the same as the number provided on a fraudulent application.

4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

   a. The address on an application is fictitious, a mail drop, or a prison; or phone number is invalid, or is associated with a pager or answering service.

5. The Social Security Number provided is the same as that submitted by other persons opening an account or other customers.

6. 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.

7. The person opening the covered account fails to provide all required personal identifying information on an application or fails to provide all the required information in response to notification that the application is incomplete.

8. Personal identifying information provided is not consistent with personal identifying information on file with the City of Dover.

9. If the City of Dover uses challenge questions, the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or credit report.

D. The unusual use of, or other suspicious activity related to, a covered account:

1. Shortly following the notice of a change of address for a covered account, the City of Dover receives a request for adding:

a. Additional properties to the account; or
b. Additional authorized users on the account.

2. A new account is used in a manner commonly associated with known patterns of fraud patterns. For example:

The customer fails to make the first payment or makes an initial payment but no subsequent payments.

3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. (Stable history shows irregularities.) For example; Nonpayment when there is no history of late or missed payments.

4. A covered account that has been inactive or has had low activity for a reasonably lengthy period of time is used or unexpectedly jumps to high consumption (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

6. The City of Dover is notified that the customer is not receiving their bills.

7. The City of Dover is notified of unauthorized charges or transactions in connection with a customer's covered account.

E. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the City of Dover:

1. The City of Dover 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.

DETECTION, PREVENTION AND MITIGATION

A. Detection

In an effort to ensure proper detection of any Red Flags, all customers must provide at least the following information/documentation before any new covered account will be opened:

1. Full Name;

2. Date of birth (individual);

3. Address, (a residential or business street address for an individual; for an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual; or for a person other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location; and;

4. Identification number, which shall be: (i) For a U.S. person, a taxpayer identification number; or (ii) For a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

   For any account holder of a covered account for which the above information is not already on file at the City of Dover, the customer will be contacted within a reasonable period of time after discovering the missing information to obtain the necessary information.

   To assist with detection of Red Flags, the City of Dover will implement the appropriate computer programs tailored to the City of Dover business needs to help authenticate customers, monitor transactions, and change of address requests.

B. Preventing and Mitigating Identity Theft

In the event a Red Flag is detected, the City of Dover is committed to preventing the occurrence of identity theft and taking the appropriate steps to mitigate any harm caused thereby. In order to respond appropriately to the detection of a Red Flag, the City of Dover shall consider any aggravating circumstance(s) that may heighten the risk of identity theft. After assessing the degree of risk posed, the City of Dover will respond to the Red Flag in an appropriate manner, which may include:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the customer;
3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
4. Reopening a covered account with a new account number;
5. Not opening a new covered account;

6. Closing an existing covered account;
7. Withholding service,
8. Not attempting to collect on a covered account or not selling a covered account to a debt collector;
9. Notifying law enforcement; or
10. Determining that no response is warranted under the particular circumstances.

All incidents and resolutions shall be tracked and documented. Internal incident form and tracking report are attached as a part of this policy.

For the protection of our customers, all service providers hired by the City of Dover to perform any activity in connection with any covered account must also take appropriate steps to prevent identity theft. To this end, the City of Dover will only contract with service providers that have implemented and follow a similar identity theft prevention policy.

TRAINING EMPLOYEES IN IDENTITY THEFT PREVENTION

A. Employees to be trained

Training will be provided to all employees that work with covered accounts and/or who handle sensitive personal identification information to enable them to detect, prevent and mitigate theft identity.

B. Training Materials

The following workbooks, which are made a part of this policy, will be used for periodic policy assessment and training tools:

1. *Identity Theft Prevention Programs in American Utilities: Guidelines for Compliance with Red Flags – Employee Workbook for Safeguarding Customer Information.*

2. *Identity Theft Prevention Programs in American Utilities: Guidelines for Compliance with Red Flags – Employee Workbook for Safeguarding Customer Information Supervisor Edition.*

PROGRAM UPDATES

The City of Dover is committed to maintaining an Identity Theft Prevention Policy that is current with the ever-changing crime of identity theft. To that end, the City will reassess this policy on an annual basis, or as necessary. In reassessing this policy, the City of Dover will add/delete Red Flags, as necessary, to reflect changes in risks to customers or to the safety and soundness of the City of Dover from identity theft. The determination to make changes to this policy will be within the discretion of the responsible parties, identified in this policy, but after careful consideration of the following:

1. The City of Dover's past experience(s) with identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent, and mitigate identity theft;

4. Changes in the types of accounts that the City of Dover offers or maintains; and

5. Changes in the business arrangements of the City of Dover, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

ADDITIONAL LEGAL REQUIREMENTS

A. Consumer Addresses

1. Address Confirmation

The City of Dover shall furnish the consumer's address that has been reasonably confirmed as accurate to credit reporting agencies as part of the information that the City of Dover regularly furnishes for the reporting period in which the City of Dover establishes a relationship with the customer. In an effort to ensure that the City maintains accurate address information for its customers and to ensure the City of Dover provides accurate address information of our customer to reporting agencies, at least one of the following steps must be taken prior to providing the customer's address to the consumer reporting agency:

a. Verify the address on file with the customer;
b. Confirm the address being sent to the credit reporting agency matches the address the City of Dover has on file for that particular customer;
c. Compare the address with information received from any third-party source; or
d. Verify by other means that are reasonably available at the time.

2. Address Discrepancies

Because the City of Dover is a user of consumer credit reports, at least one of the following steps must be taken when the City receives notice from any credit reporting agency that a substantial difference exists between the address for the customer that the City of Dover provided and the address(es) in the credit reporting agency's file for that particular customer:

a. Compare the differing address with the City of Dover 's file, by either (1) confirming that the address information provided by the City to the credit reporting agency is the same information the City of Dover obtains and uses to verify the customer's identity in accordance with the requirements of the Customer Information Program (CIP) rules (31 USC 5318(1) (31 CPR 103.121»; or (2) comparing the differing addresses with the City of Dover records and files, including applications, change of address notifications, other customer account records, or retained CIP documentation; or (3) comparing the differing addresses with information the City of Dover may have received from a third-party source; or
b. Verify the information in the credit report provided by the credit reporting agency with the customer.

B. Other requirements should be addressed below based on entity type

Examples:

a. Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2 (Fair Credit Reporting Act, which imposes responsibilities on all persons who furnish information to consumer reporting agencies), for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and
b. Complying with 15 U.S.C. l681m, of the Fair Credit Reporting Act, which prohibits the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Consumer ID Theft Incident Report

(for internal use only)

Victim Information

1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

2) (If different from above) When the events described in this affidavit took place I was known as _____
_____
(First) (Middle) (Last) (Jr., Sr., III)

3) My date of birth is _____
(day/month/year)

4) My Social Security number is _____

5) My driver's license or identification card state and number are _____

6) My current address is _____

City _____ State _____ Zip Code _____

7) I have lived at this address since _____
(month/year)

8) (If different from above) When the events described in this affidavit took place, my address was _____
_____

City _____ State _____ Zip Code _____

9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

10) My daytime telephone number is (_____) _____
My evening telephone number is (_____) _____

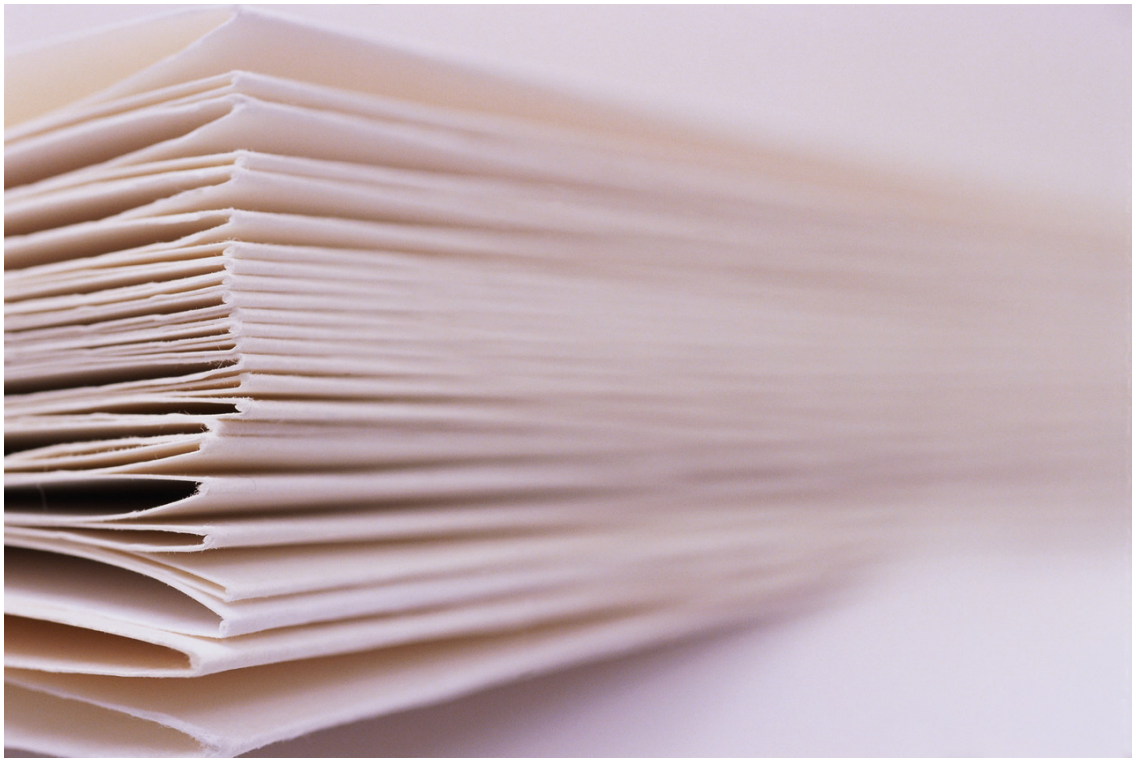
City of Dover

Identity Theft Prevention Tracking Report

Date	Scope	Employee	Employee Trained	Describe Incident or "Significant Event"	Management Response	Mitigation

(FOR INTERNAL USE ONLY)

Identity Theft Prevention Programs in American Utilities: Guidelines for Compliance with Red Flags



Provided by Tennessee Valley Public Power Association

Employee Workbook for Safeguarding Customer Information

Dedication

This program is dedicated to the thousands of utility workers who relentlessly serve. You do not get to choose who will be your customer. As a result, you serve all sides of humanity. The kindness and respect you show to those, who have not been so generous with you, is perhaps your most remarkable accomplishment of all.

Red Flags Employee Training

It Takes a Thief

To begin this training, you are going to look at the world through the eyes of a criminal. Imagine being in and around your utility on the lookout for secured information (Social Security Number-SSN, driver's license, Date of Birth-DOB, address, name, etc.). You have a notebook and a brief case. Let's see what you can find.

In the parking lot, you find an unlocked company vehicle with a laptop. Quickly, stick it in your briefcase. You overhear a customer at the drive up window tell the CSR his name, address, and date of birth. The CSR repeats the information back to him. You have written it down in your notebook. Good work. A look around the dumpster reveals half of a crumpled application that has what looks like coffee on it. On the barely readable paper is a name, address, date of birth, social security number and place of employment. Now you are getting somewhere. Take this stuff home. You have too much to run a risk. From a phone at the customer's place of employment, call the bank and ask about last payment. "I think I might have paid that bill twice – What is the last check number you show? My husband keeps so many accounts. Is that the First American Account or Regency Bank?"

This is just too much fun. Now you are going back to see what you can find when you go inside the doors. First, write down any information in the area where new accounts are opened. If the CSR leaves his desk, look in the trashcan for notes, on the desk for files and quickly put them in your brief case. If there are any access codes or passwords taped or on a sticky note on the monitor, write them down in your notebook. You have a buyer for that stuff. Search any area for abandoned monitors that still have social security information on the screen. Hey wait this desk has the access code numbers taped under the work area. Who do they think they're kidding? It just does not get better than this. Now let's look for purses. It takes a little time, but you just found the purse of a new employee. Wow, real leather; at least our victim has nice taste.

Back at home camp, you check inside the purse: a cell phone, driver's license, social security card, ATM card, checkbook and pictures. You text her husband saying, "I forgot the pin number!" If he gives it to you, respond thanks and celebrate. You have just completed your first morning of life as a thief. Not bad.

In order to protect our customers from identity theft, we have to be one step ahead of thieves. In each of the above situations, how could the utility employees better protect the information?

Introduction:

In the time it takes to read this first sentence there will be four (4) new victims of identity theft in the United States.

The fastest and most financially devastating crime in the United States is identity theft. The emotional and financial cost to the victim can affect their quality of life. In a utility, breaches in information security, lessen the trust the public must place on us to establish the power supplier/consumer relationship.

I. How Legislation is Changing the Way We Monitor and React to Possible Signs of Identity Theft or Red Flags.

The FACT Act (2003) was passed to set standards for guarding customer information. On November 1, 2007, the red flags were added to hold businesses liable for the prevention, detection and mitigation of identity theft.

Does your utility daily procedures support consumer privacy?

A. *Why Utilities?*

- Because utilities maintain on going accounts primarily for personal, family or household purposes.
- The accounts are designed to accept multiple payments.
- Utilities are the site for a large portion of identity theft crime in the United States.

B. *Are We Responsible to Our Members/Customers?*

In a word, yes. The utility has the responsibility of developing an identity theft prevention program to protect our customer's personal information. The FACT Act outlines the requirement to:

DETECT

PREVENT

MITIGATE[1]

C. *Where Do We Begin?*

- Make a list of red flag indicators of identity theft drawn from experience in the utility industry. In other words, what has been the past and current patterns used to gain services under a stolen identity?
- What proactive strategies can be incorporated into our day to day policies and procedures that will discourage or detect identity thieves?

[1] Control damage done

D. *How Do We Add One More Thing On Our Plate?*

In the utility industry, a strong sense of providing reliable service has always been evident. We provide a critical service that our customers need to sustain everyday life. The dedication to protecting and serving "the little lady at the end of the line" has always been a part of out culture.

The Identity Theft Prevention Program is another step in the direction of providing service for our customers. Protecting a customer's personal identity information is indeed our lawful responsibility.

Effective business practices and policies that spot attempted and actual identity theft early have great potential for relieving the national crime wave. Identity thieves often establish cell phone and utility (established proof of residency) accounts in the victim's name.

Utilities suffer significant losses from customers who use stolen identities for service and walk away from large bills. Careful validation of identity in the process of opening an account and the use of red flags (such as alerts) has already been demonstrated to minimize losses. Proper screening of new and existing accounts not only protects secure information but also is an effective approach to keeping the cost per kilowatt-hour within reach of the working family.

What is a red flag?

A pattern, particular specific activity that indicates the possible risk of identity theft.

A red flag triggers the need to investigate, gather facts and mitigate.

Examples:

It is important that red flags be treated as examples of indicators of possible theft and not defacto evidence of identity theft.

- A consumer fraud alert or active duty alert
- Any account that would adversely affect a consumers credit standing should be considered at risk of identity theft and thus subject to a red flag
- An address discrepancy reported by a consumer reporting agency
- A consumer's communication about attempted or actual identity theft
- A company's knowledge of a security breach within it's own confines or that of an affiliate with which the company has shared data
- Attempts to open new accounts with altered documents
- Suspicious actions by employees – downloading customer account information being added to customer account

The vast majority of identity theft in the utility industry has historically been within families. There is no reason to doubt that trend will still occur. There is, however, a much more dangerous threat developing throughout the US. Professional or maybe we should just say very effective thieves, will usually establish proof of residency with a

utility bill. Our government is asking us to not only protect our customer's secured information, but be a part of the answer to the problem. Remember, *it is not our job to accuse, only to report. Being consistently kind and respectful is always the right thing to do. This will keep make the environment safer for us and we will be less likely to accuse someone who is innocent. You may also find that the detective or police officer in your area does not want a potential suspect to be forewarned.*

E. *Identity Theft versus Identity Fraud*

Identity fraud occurs when someone gives you fictitious information such as:

- a social security number that has never been issued.
- an address that does not exist.
- the name of a person that does not exist.

In this case the utility has the option to respectfully request additional before beginning services. A potential victim has not been established.

Identity theft occurs when someone gives you fraudulent information such as:

- social security number issued to another individual.
- social security number listed on death file.
- name and address belonging to someone else.

In this case, the suspicion of a potential victim has been established.

Identity theft is a much more serious problem. Identity theft is when someone gathers personal information and assumes a new identity as their own. This can include getting seemingly authentic forms of identification using real or fake "breeder" documents (a breeder document is a document used to establish identity for other forms of ID; for example, presenting a birth certificate to the department of motor vehicles to get a drivers license). With their new identification in hand, criminals perpetrating an actual identity theft can then open new accounts, apply for loans or mortgages, and generally make a very big, expensive mess of the victim's life.

Case No. 1

Title: "Stolen Identity"

In the public power industry, over 50% of all identity theft occur within families.

A sister in Middle Tennessee used a social security number that belonged to her sister that lived in Kentucky. She is able to obtain fraudulent picture identification in her sister's name. She opens a new water, gas, electric and cable account at the local municipality. While she paid the initial deposit, her bills are being returned by the post office. She has made no attempt to make any payment at 60 days. A service man is sent to warn her about the cut off date and tells him she would be more than happy to pay. She explains she needs the bills in writing because her father in Texas is paying them for her. The accounting office grants her an additional 30 days to complete all transactions with the condition that all accounts will be current by the 10th of the month. On the 8th, she has a church organization working to help her raise the funds. On the 11th, the sister in Kentucky sees the activity on her credit report. Her sister has had a life long habit of manipulating family members to survive. For years they followed her from state to state cleaning up the mess. The sister in Kentucky calls the utility and alerts them of the fraudulent use of her identity.

Topics of Discussion:

1. How would you verify the facts? How will we establish "reasonable basis" for identity?

2. When you have confirmed that she has stolen her sister's identity, how will you proceed?

Case No. 2

Title: *Mrs. B*

Mrs. B sent her 10 year old grandson, John, a check for his birthday. John's parents have recently divorced on bad terms. His father sees the check in John's book bag on a scheduled visit and copies down the routing number and checking account number. He uses the information to call in utility payments for the next three months. Mrs. B realizes the theft when her sister comes by to help her manage her account. She is embarrassed, by her former son-in-law's behavior, but does not want to be held accountable for the $721.00 in charges and late fees. The Utility is notified of the son in law's intent of fraudulent use of Mrs. B's banking account.

Topics of Discussion:

1. Could this theft have been detected before Mrs. B. called? How?

2. Do you think it is possible that Mrs. B has cleaned up the financial messes made by this man before?

3. How should the Utility handle the current situation?

4. What can the Utility do to prevent a repetition?

F. *Red Flags Checklist and Review for Utilities*

Alerts, Notifications or Warnings from Consumer Reporting Agency	Suspicious Documents	Suspicious Personal I.D. Information	Unusual Use or Suspicious Activity related to the Covered Account	Notice of Theft
1. A fraud or active duty alert is included with a consumer report.	5. Documents provided for ID appeared altered or forged	10. Personal ID is inconsistent with external information sources: addresses do match consumer report/ or social security (SS) number has not been issued or is listed on the SS Administration Death Master File	19. Change of billing address is followed by request for adding additional properties to the account (or shortly following the notification of a change in address, the utility receives a request for the addition of authorized users on the account.)	26. Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.
2. Consumer reporting agency provides a credit freeze on the customer report	6. The photo or physical description is not consistent with the appearance of the applicant	11. Personal ID given by customer is not consistent with other personal ID info. Ex: There is a lack of correlation between the SSN# range and DOB	20. Payments are made in a manner associated with fraud. For example, deposit or initial payment is made and no payments are made thereafter.	
3. Consumer Reporting Agency provides a notice of address discrepancy	7. Other information given to open the new account is not consistent with the ID of the applicant	12. Personal ID provided is associated with known fraudulent activity. Using same addresses and or phone numbers	21. Existing account with a stable history shows irregularities	
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer such as :	8. Other information on the identification is not consistent with readily accessible info on file such as signature or recent check.	13. Personal ID is of the same type associated with fraudulent activity: fictitious address, mail box drop, or prison or phone number is invalid; it is associated with a pager or answering service.	22. An account with low activity unexpectedly jumps to high consumption.	
a. recent or significant increase in the number of inquiries	9. An application appears to have been altered or forged, or gives the appearance or having been destroyed and reassembled.	14. The SS# is the same as customers opening other accounts.	23. Mail sent to customer is repeatedly returned.	
b. an unusual number of recently established credit relationships		15. The address or phone number is the same as a large number of other applicants.	24. Customer notifies utility that they are not receiving their bill.	
c. a material change in the use of credit especially with respect to new established credit relationships		16. The customer fails to provide all needed personal ID upon request.	25. The utility is notified of unauthorized charges or transactions in connection with a customer's account.	
d. an account that was closed for cause or identified for abuse of account privileges		17. Personal ID is inconsistent with utility records.		
		18. For institutions using challenge questions, the person attempting to access or open the account cannot provide any information beyond what would typically be found in a wallet or consumer report		

Step 1 – Map out the steps that occur for processing a new account.

Customer Initial Contact

Service is Established

After you have mapped out the steps in gathering customer information to start a new account, highlight the areas where red flags might possibly appear.

Step 2 - Map out the ways customers, 3rd parties and others access existing accounts.

Request

Request Fulfilled

After you have mapped out the flow of information, highlight the possible areas where a red flag could occur.

Discuss with your supervisor, what is the policy in you utility in the event of:

	Employee Responses Include:
Alerts:	
• Fraud • Credit Freeze • Notice of Address Discrepancy • Unusual Pattern of Activity	
Suspicious Documents:	
• ID altered or Forged • Photo or description does not match customer • Inconsistent information • Paperwork appears to have been forged or altered, destroyed and reassembled	
Suspicious Personal ID Information:	
ID inconsistent with external sources: • Address does not match consumer report • SS# given has not been listed or is on the SS Adm. Death Master File • ID info conflicts such as SS# and DOB Information given is associated with fraudulent activity • SSN is same as other customers • Address is same as other customers • Customer fails to provide all ID requested • Personal ID is inconsistent with utility records	
Unusual Use or Suspicious Activity:	
• Change of billing address is followed by authorization of additional users • Deposit is made and no payments are made there after • An existing account with a stable history shows irregularities • Mail sent to customer is repeatedly returned • Customer notifies utility that they are not receiving their bill	

Notice of theft:	
• Utility is notified of unauthorized charges or transactions in connection with a customer's account	

Case No. 3

Title: *Kentucky Consumer*

"My 9 year old daughter was a victim of identity theft through this organization. Someone used my daughter's Social Security Number to obtain unauthorized utilities in her name. (The) utility was unwilling to assist in my daughter's case in bringing the perpetrator to justice. The (utility company) informed me that they do not run checks on identification showed to them to ensure validity. The (utility company) informed me that it is easier and cheaper to write off utility losses then to investigate and prosecute cases of utility fraud/identity theft. I feel that this exemplifies poor public security and displays ineptness towards individual rights. My daughter was a victim and I am sure there are many more that will be victimized as long as companies refuse to stand up for laws that protect us." (This story posted online on 9/22/04)

Topics of Discussion:

1. Why do you think utilities tend to write off losses vs. investigate and prosecute?

2. Why are children a target for stolen social security numbers?

3. Does the customer have a right to feel "protected?"

What is your role in the utility's identity theft prevention program?

Due diligence with regard to protecting customer information

This includes your own daily habits:

- ✓ Disposing of records or paper with notes
- ✓ Taping access information around work station
- ✓ Speaking in a manner that allows others to overhear secured information
- ✓ Leaving your work area with the monitor on, files on desk, customer information in view of others
- ✓ Sharing passwords, access codes, etc
- ✓ Discussing personal information regarding a customer with other employees. Information is shared only on a "Need to Know" basis.

Carefully monitor your work area

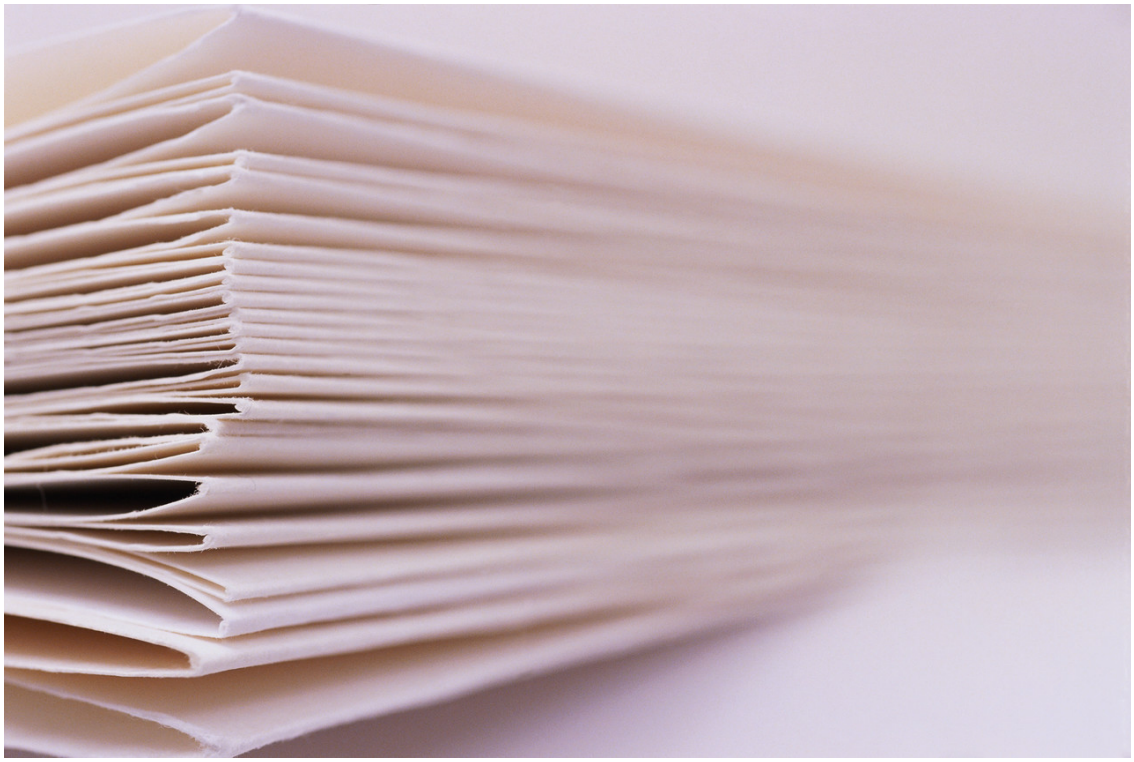
If someone implies they are with an outside vendor authorized to access your equipment, verify first with your supervisor.

Watch for unusual behavior, employees downloading large amounts of information, unauthorized personnel or citizens in areas with secured information.

Validate identification for new and existing accounts. Check documents. Our customers do have a right to feel protected.

Utility employees are not required or encouraged to confront individuals suspected of committing a crime. It is our lawful obligation to report to the police any "suspected" patterns of identity theft. It is the responsibility of the detective or officer working in identity theft to do the investigation. The laws regarding reporting identity theft are similar to reporting child abuse. You report when there is a suspicion. It is up to law officials to determine if a crime has actually been committed.

Identity Theft Prevention Programs in American Utilities: Guidelines for Compliance with Red Flags



Provided by Tennessee Valley Public Power Association

Employee Workbook for Safeguarding Customer Information Supervisor Edition

Dedication

This program is dedicated to the thousands of utility workers who relentlessly serve. You do not get to choose who will be your customer. As a result, you serve all sides of humanity. The kindness and respect you show to those, who have not been so generous with you, is perhaps your most remarkable accomplishment of all.

Forward

This program has been designed to address the training needs in the utility industry regarding identity theft prevention. Under the revisions to the FACT Act 2003 (Fair and Accurate Credit Transactions Act), each utility is required to have policies and procedures in place by November 1st, 2008 which meet the standards outlined by Federal Agencies including the U. S. Department of Treasury . There are 31 red flags included in the current legislation. Portions of these occur more frequently in utilities than others. The proposed training takes the regulations and translates the language into practical case studies using real life utility situations. The target audience includes management and staff from accounting, human resources, IT, risk management, administration and other key personnel.

Red Flags Employee Training

It Takes a Thief

To begin this training, you are going to look at the world through the eyes of a criminal. Imagine being in and around your utility on the lookout for secured information (Social Security Number-SSN, driver's license, Date of Birth-DOB, address, name, etc.). You have a notebook and a brief case. Let's see what you can find.

In the parking lot, you find an unlocked company vehicle with a laptop. Quickly, stick it in your briefcase. You overhear a customer at the drive up window tell the CSR his name, address, and date of birth. The CSR repeats the information back to him. You have written it down in your notebook. Good work. A look around the dumpster reveals half of a crumpled application that has what looks like coffee on it. On the barely readable paper is a name, address, date of birth, social security number and place of employment. Now you are getting somewhere. Take this stuff home. You have too much to run a risk. From a phone at the customer's place of employment, call the bank and ask about last payment. "I think I might have paid that bill twice – What is the last check number you show? My husband keeps so many accounts. Is that the First American Account or Regency Bank?"

This is just too much fun. Now you are going back to see what you can find when you go inside the doors. First, write down any information in the area where new accounts are opened. If the CSR leaves his desk, look in the trashcan for notes, on the desk for files and quickly put them in your brief case. If there are any access codes or passwords taped or on a sticky note on the monitor, write them down in your notebook. You have a buyer for that stuff. Search any area for abandoned monitors that still have social security information on the screen. Hey wait this desk has the access code numbers taped under the work area. Who do they think they're kidding? It just does not get better than this. Now let's look for purses. It takes a little time, but you just found the purse of a new employee. Wow, real leather; at least our victim has nice taste.

Back at home camp, you check inside the purse: a cell phone, driver's license, social security card, ATM card, checkbook and pictures. You text her husband saying, "I forgot the pin number!" If he gives it to you, respond thanks and celebrate. You have just completed your first morning of life as a thief. Not bad.

In order to protect our customers from identity theft, we have to be one step ahead of thieves. In each of the above situations, how could the utility employees better protect the information?

Introduction:

In the time it takes to read this first sentence there will be four (4) new victims of identity theft in the United States.

The fastest and most financially devastating crime in the United States is identity theft. The emotional and financial cost to the victim can affect their quality of life. In a utility, breaches in information security, lessen the trust the public must place on us to establish the power supplier/consumer relationship.

I. How Legislation is Changing the Way We Monitor and React to Possible Signs of Identity Theft or Red Flags.

The FACT Act (2003) was passed to set standards for guarding customer information. On November 1, 2007, the red flags were added to hold businesses liable for the prevention, detection and mitigation of identity theft.

Does your utility daily procedures support consumer privacy?

A. *Why Utilities?*

- Because utilities maintain on going accounts primarily for personal, family or household purposes.
- The accounts are designed to accept multiple payments.
- Utilities are the site for a large portion of identity theft crime in the United States.

B. *Are We Responsible to Our Members/Customers?*

In a word, yes. The utility has the responsibility of developing an identity theft prevention program to protect our customer's personal information. The FACT Act outlines the requirement to:

DETECT

PREVENT

MITIGATE[1]

C. *Where Do We Begin?*

- Make a list of red flag indicators of identity theft drawn from experience in the utility industry. In other words, what has been the past and current patterns used to gain services under a stolen identity?
- What proactive strategies can be incorporated into our day to day policies and procedures that will discourage or detect identity thieves?

[1] Control damage done

D. *How Do We Add One More Thing on Our Plate?*

In the utility industry, a strong sense of providing reliable service has always been evident. We provide a critical service that our customers need to sustain everyday life. The dedication to protecting and serving "the little lady at the end of the line" has always been a part of out culture.

The Identity Theft Prevention Program is another step in the direction of providing service for our customers. Protecting a customer's personal identity information is indeed our lawful responsibility.

Effective business practices and policies that spot attempted and actual identity theft early have great potential for relieving the national crime wave. Identity thieves often establish cell phone and utility (established proof of residency) accounts in victim's name.

Utilities suffer significant losses from customers who use stolen identities for service and walk away from large bills. Careful validation of identity in the process of opening an account and the use of red flags (such as alerts) has already been demonstrated to minimize losses. Proper screening of new and existing accounts not only protects secure information but also is an effective approach to keeping the cost per kilowatt-hour within reach of the working family

What is a red flag?

A pattern, particular specific activity that indicates the possible risk of identity theft.

A red flag triggers the need to investigate, gather facts and mitigate.

Examples:

It is important that red flags be treated as examples of indicators of possible theft and not defacto evidence of identity theft.

- A consumer fraud alert or active duty alert
- Any account that would adversely affect a consumers credit standing should be considered at risk of identity theft and thus subject to a red flag
- An address discrepancy reported by a consumer reporting agency
- A consumer's communication about attempted or actual identity theft
- A company's knowledge of a security breach within it's own confines or that of an affiliate with which the company has shared data
- Attempts to open new accounts with altered documents
- Suspicious actions by employees – downloading customer account information being added to customer account

E. *Identity Theft versus Identity Fraud*

Identity fraud occurs when someone gives you fictitious information such as:

- a social security number that has never been issued.
- an address that does not exist.
- the name of a person that does not exist.

In this case the utility has the option to respectfully request additional information before beginning services. A potential victim has not been established.

Identity theft occurs when someone gives you fraudulent information such as:

- social security number issued to another individual.
- social security number listed on death file.
- name and address belonging to someone else.

In this case, the suspicion of a potential victim has been established.

Identity theft is a much more serious problem. Identity theft is when someone gathers personal information and assumes a new identity as their own. This can include getting seemingly authentic forms of identification using real or fake "breeder" documents (a breeder document is a document used to establish identity for other forms of ID; for example, presenting a birth certificate to the department of motor vehicles to get a drivers license). With their new identification in hand, criminals perpetrating an actual identity theft can then open new accounts, apply for loans or mortgages, and generally make a very big, expensive mess of the victim's life.

Case Studies in Utilities
Identity Theft Prevention Program

Case No. 1

Title: "Stolen Identity"

In the public power industry, over 50% of all identity theft occur within families.

A sister in Middle Tennessee used a social security number that belonged to her sister that lived in Kentucky. She is able to obtain fraudulent picture identification in her sister's name. She opens a new water, gas, electric and cable account at the local municipality. While she paid the initial deposit, her bills are being returned by the post office. She has made no attempt to make any payment at 60 days. A service man is sent to warn her about the cut off date and tells him she would be more than happy to pay. She explains she needs the bills in writing because her father in Texas is paying them for her. The accounting office grants her an additional 30 days to complete all transactions with the condition that all accounts will be current by the 10th of the month. On the 8th, she has a church organization working to help her raise the funds. On the 11th, the sister in Kentucky sees the activity on her credit report. Her sister has had a life long habit of manipulating family members to survive. For years they followed her from state to state cleaning up the mess. The sister in Kentucky calls the utility and alerts them of the fraudulent use of her identity.

Topics of Discussion:

1. How would you verify the facts? How will we establish "reasonable basis" for identity?

2. When you have confirmed that she has stolen her sister's identity, how will you proceed?

Case Studies in Utilities
Identity Theft Prevention Program

Case No. 2

Title: *Mrs. B*

Mrs. B sent her 10 year old grandson, John, a check for his birthday. John's parents have recently divorced on bad terms. His father sees the check in John's book bag on a scheduled visit and copies down the routing number and checking account number. He uses the information to call in utility payments for the next three months. Mrs. B realizes the theft when her sister comes by to help her manage her account. She is embarrassed, by her former son-in-law's behavior, but does not want to be held accountable for the $721.00 in charges and late fees. The Utility is notified of the son in law's intent of fraudulent use of Mrs. B's banking account.

Topics of Discussion:

1. Could this theft have been detected before Mrs. B. called? How?

2. Do you think it is possible that Mrs. B has cleaned up the financial messes made by this man before?

3. How should the Utility handle the current situation?

4. What can the Utility do to prevent a repetition?

F. *Red Flags Checklist and Review for Utilities*

Alerts, Notifications or Warnings from Consumer Reporting Agency	Suspicious Documents	Suspicious Personal I.D. Information	Unusual Use or Suspicious Activity related to the Covered Account	Notice of Theft
1. A fraud or active duty alert is included with a consumer report.	5. Documents provided for ID appeared altered or forged	10. Personal ID is inconsistent with external information sources: addresses do not match consumer report/ or social security (SS) number has not been issued or is listed on the SS Administration Death Master File	19. Change of billing address is followed by request for adding additional properties to the account (or shortly following the notification of a change in address, the utility receives a request for the addition of authorized users on the account.)	26. Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.
2. Consumer reporting agency provides a credit freeze on the customer report	6. The photo or physical description is not consistent with the appearance of the applicant	11. Personal ID given by customer is not consistent with other personal ID info. Ex: There is a lack of correlation between the SSN# range and DOB	20. Payments are made in a manner associated with fraud. For example, deposit or initial payment is made and no payments are made thereafter.	
3. Consumer Reporting Agency provides a notice of address discrepancy	7. Other information given to open the new account is not consistent with the ID of the applicant	12. Personal ID provided is associated with known fraudulent activity. Using same addresses and or phone numbers	21. Existing account with a stable history shows irregularities	
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer such as :	8. Other information on the identification is not consistent with readily accessible info on file such as signature or recent check.	13. Personal ID is of the same type associated with fraudulent activity: fictitious address, mail box drop, or prison or phone number is invalid; it is associated with a pager or answering service.	22. An account with low activity unexpectedly jumps to high consumption. Ex: 1000 kwh to 2801 kwh.	
a. recent or significant increase in the number of inquiries	9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.	14. The SS# is the same as customers opening other accounts.	23. Mail sent to customer is repeatedly returned.	
b. an unusual number of recently established credit relationships		15. The address or phone number is the same as a large number of other applicants.	24. Customer notifies utility that they are not receiving their bill.	
c. a material change in the use of credit especially with respect to new established credit relationships		16. The customer fails to provide all needed personal ID upon request.	25. The utility is notified of unauthorized charges or transactions in connection with a customer's account.	
d. an account that was closed for cause or identified for abuse of account privileges		17. Personal ID is inconsistent with utility records. 18. For institutions using challenge questions, the person attempting to access or open the account cannot provide any information beyond what would typically be found in a wallet or consumer report		

G. *Needs Assessment*

Opening a New Account

Identify the steps in establishing electrical service for a customer.

1) What identification is required? How do you obtain identifying information and verify identity? _____

2) Do they need to make the application in person or can they send in the information in an alternate form? Telephone or other? _____

3) Does the utility use consumer reports in the application process? How? Establish deposit? Approve or deny services? _____

4) Does the utility have policies and procedures that define red flags for identity theft and actions for mitigation? (See *Taking the Right Step*) _____

5) What happens to the hand written notes made by the CSR in the application process? _____

6) Is the computer screen visible to others during the application process? _____

7) Who has access to data once entered? Does the CSR lock computer when not at desk? _____

8) If applicant gives address, bank account, date of birth or social security number verbally to CSR, what precautions are taken from others hearing? _____

9) Once personal identification information is entered by CSR, where and how can it later be retrieved?_____ _____What safe guards are currently built into the application process? _____ _____ _____

10) What safeguards would you like to implement? _____ _____ _____ _____

11) Which employees have access to information – is it on a "need to know" basis? _____ _____ _____ _____

12) Is any customer personal information carried into the field on a laptop? _____ _____ _____ _____

Step 1 – Map out the steps that occur for processing a new account.

Customer Initial Contact

Service is Established

Are there any areas where you can improve security of information?

H. *Monitoring Existing Account*

Identify the possible red flags, which may exist in the following procedures:

- ✓ Authenticating transactions for existing customers
- ✓ Payments made by check, credit cards, debit card, etc.
- ✓ Verifying the validity of change of billing address
- ✓ Does the utility have policies and procedures that define red flags for identity theft and action for mitigation for existing accounts?

Use of Passwords - Security Access

_____
_____
_____
_____

What safeguards are currently built into monitoring existing utility accounts?

_____
_____
_____
_____

Step 2 - Map out the ways customers, 3rd parties and others access existing accounts.

Request

Request Fulfilled

Highlight any areas where you feel it is possible to provide further protection for secured information.

I. *Taking the Right Step/Designing the Policies for Your Utility*

Utility employees are not required or encouraged to confront individuals suspected of committing a crime. It is our lawful obligation to report to the police any "suspected" patterns of identity theft. It is the responsibility of the detective or officer working in identity theft to do the investigation. The laws regarding reporting identity theft are similar to reporting child abuse. You report when there is a suspicion. It is up to law officials to determine if a crime has actually been committed.

Every case will have various factors, but as a rule, how do you want the employees in your utility to proceed when presented with the following red flags? As you complete the chart on the following pages, choices for possible mitigation are listed in the box below.

Choices for Mitigation

Under the third column, consider choices from the following options:

a) Monitoring account for evidence of identity theft;
b) Contacting the customer;
c) Changing any passwords, security codes, or other devices that permit access to a covered account;
d) Reopening an account with a new account number;
e) Not opening a new account;
f) Closing an existing account;
g) Not attempting to collect on an account or not selling a covered account to a debt collector;
h) Notifying law enforcement; or
i) Determining that no response is warranted under the particular circumstances

Flag	**Next Step**	**Mitigation** (Steps to Control Losses)
Alerts		
Consumer report indicates fraud or active duty alert.		
Credit freeze.		
Notice of address discrepancy.		
Unusual patterns in activity.		
Presentation of Suspicious Documents		
Identification documents appear altered or forged.		
Photo/physical description does not match applicant.		

Flag	Next Step	Mitigation (Steps to Control Losses)
Other information on identification is inconsistent information given from applicant.		
Information in utility files in inconsistent with information provided. Example – signatures do not match on signature card.		
Application looks altered or forged or destroyed and reassembled.		
Suspicious Personal Identifying Information		
Identification is inconsistent with external source such as: - Address v. Address on Consumer Report - Social security number not issued. - Social security number on Death Master file. - Inconsistent information, such as lack of correlation between date of birth and social security number.		
Identification is known to be associated with fraudulent activity: - The address is fictitious, a prison or a mail drop on application. - The phone number is invalid or associated with a pager or answering service. - The social security number is the same as that submitted by other persons opening an account.	**Note: How will you distinguish customers who own rental property, barns, etc. and have multiple accounts under the same information?**	

Flag	Next Step	Mitigation (Steps to Control Losses)
- The address is the same address as that submitted by other persons opening an account.		
Applicant fails to provide all personal ID requested.		
Personal ID is inconsistent with utility records.		
For institutions using challenge questions, the person attempting to access or open the account can not provide any information beyond what would typically be found in a wallet or consumer report.		
Change of billing address is followed by request for adding additional properties to the account (or shortly following the notification of a change in address, the utility receives a request for the addition of authorized users on the account).		
Payments are made in a manner associates with fraud. For example, deposit or initial payment is made and no payments are made thereafter.		
Existing account with a stable history shows irregularities.		
An account with low activity unexpectedly jumps to high consumption. Ex: 1000 kwh to 2801 khw.		
Mail sent to customer is repeatedly returned.		
Customer notifies utility that they are not receiving their bill.		

Flag	Next Step	Mitigation (Steps to Control Losses)
The utility is notified of unauthorized charges or transactions in connection with a customer's account.		
Notice of Theft		
Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.		

J. *Disposal of Secure Information*

Utilities will need to be able to prove that they have destroyed sensitive documents or information to be FACT Act compliant. This requires documentation of what and when information was destroyed.

Utilities need a written program outlining how to maintain and shred documents and destroy data:

- ✓ Well-defined step by step procedures for handling various types of data and documents.
- ✓ Procedures for collecting and protecting documents and data until the time of destruction.
- ✓ Documentation of Record Destruction.

Best Practices:

- ✓ Placing shredders next to trash cans and copiers enhance employee compliance.
- ✓ Transfer shredded documents to a locked bin until the documents can be destroyed.
- ✓ Under the FACT Act, samples of destruction of data includes, pulverizing or burning paper and erasing electronic data.
- ✓ Train CSRs and any other employees who at times make hand written notes to destroy after data is entered.
- ✓ Keep your own records of data destruction, even if you use a outside contractor, you are still ultimately responsible.

Schedules for Data and Document Disposal
Regularly scheduled paper shredding and data disposal is recommended to prevent liability from storing excess records with personal information. A documented procedure and schedule will show consistency in action and intent.

Case Studies in Utilities
Identity Theft Prevention Program

Case No. 3

Title: ***Missouri Consumer***

"A computer was purchased illegally using my name, date of birth, and social security number. (A detective) from the Minneapolis Police and (a detective) from the Kansas City Police filed identity theft reports and initiated investigations. (One of the detectives and) I contacted (the computer company) numerous times for serial and model numbers of the computer delivered to residents in Minneapolis. A warrant will be issued for the arrest of the thieves if this information is provided. (The computer company's) Fraud Department has not fully cooperated in giving correct information. I am planning to file a lawsuit against (the computer company) for obstructing this investigation. Also, I will contact the Attorney General's Office in (a third state) for an investigation. It is very suspicious that (the computer company) refuses to assist. Perhaps, a (company) employee or department is attempting to cover up some questionable practices." (This story posted online on 09/07/04)

Topics of Discussion:

1. How could an employee or group of employees in the computer company be involved in questionable practices?

2. What are the best strategies to prevent criminal behavior within the utility staff?

3. What does the term "need to know" basis mean?

Case Studies in Utilities
Identity Theft Prevention Program

Case No. 4

Title: ***Family Service Disconnected for Non Payment***

In May 2005, a house fire in Hastings, PA killed an adult and three children under the age of 18. The home had been without electricity for four days due to a disconnection of service by Penelec. The fire started with a candle. This incident resulted in widespread news accounts and reportings on the changes to Pennsylvania's consumer protection policies as a result of the adoption of Chapter 14 and the significant increase in utility disconnections and adoption of more strict payment requirements, as well as the reduction in efforts for personal contact and renegotiation of payment arrangements. The Commission opened an investigation of this disconnection and is considering a settlement of the investigation that would require the utility to pay an additional $250,000 to its low income assistance fund and adopt changes to its termination practices, including procedures relating to the explanations of medical certification information on its notices, and restoration practices upon receipt of a valid medical certification.

Topics of Discussion:

1. What are the social issues that surround the utility industry?

2. How is our service different from the other industries covered in the FACT Act? Banks, Credit Unions, etc.

Conclusion

As a supervisor, your role in the utility identity theft prevention program involves:

***Learning the specific procedures for handling the various red flags in your utility.**

- Restrict access to information on a need to know basis. Set your employees up to succeed by teaching them how to handle difficult situations before they occur. Train Train and then Train some more
- Monitor for an employee breech in security-Know what the signs would look like in your area
- Teach employees to deny access to anyone to computers, files, secured information without consulting with you.
- Do regular walk through audits in your own department.
- Carefully screen all new hires.
- Know the privacy officer and identity theft prevention committee.
- Keep a record of all incidents. The privacy officer will use this data to study strategies to improve your program.
- Help your employees understand the need to be kind and respectful to everyone. Thankfully, it is not our job to convict. We only note the red flags as they occur and report as our procedure dictates.

The vast majority of identity theft in the utility industry has historically been within families. There is, however, a much more dangerous threat developing throughout the US. Professional or maybe we should just say very effective thieves, will usually establish proof of residency with a utility bill. Our government is asking us to not only protect our customer's secured information, but be a part of the answer to the problem.

***Remember**, it is not our job to accuse, only to report. Being consistently kind and respectful is never the wrong thing to do.*