Division of Accounting – Policies and Procedures Manual Standard Policies and Procedures	
Policy Number: AUB-05-13	Revision Number: 1
	Effective Date: 10-01-2023
Subject: Fair and Accurate Credit Transactions Act (FACTA) Compliance	Privacy Officer Approval:
	General Manager Approval:

- **Purpose**

Utilities in Tennessee must abide by the Fair and Accurate Credit Transactions Act (FACTA). This act requires that most creditors (including municipal utilities by definition) develop a documented program designed to detect, prevent, and mitigate identity theft in connection with the opening of an account or an existing account. This policy and procedure will serve to document the Athens Utilities Board's program and compliance with the requirements of the FACTA.

- **References**

(1) "Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003; Final Rule" - Federal Register, Volume 72, Number 217, Friday, November 9, 2007

- **Definitions**

AUB – means the Athens Utilities Board, and its duly authorized employees, agents, and representatives
Board – means the Chairman and all Commissioners but does not include any employees
Customer – Any person, business, or other entity that receives electrical service from Athens Utilities Board, Division of Power
Division – The Athens Utilities Board, division of Power, Water, wastewater, or gas
FACTA – Fair and Accurate Credit Transactions Act
IDT – Identity Theft

4.0 Identity Theft Prevention Plan

The Identity Theft Prevention Plan lays out the basic steps that will be taken by AUB to prevent, identify, and mitigate IDT consistent with the purpose of FACTA and to protect our customer base from IDT.

The Identity Theft Plan is included in this Policy and Procedure as Attachment PP AUB-05-11-A1

- **Designation of Privacy Officer**

As required by FACTA, AUB has designated the General Manager as the current privacy officer responsible for the establishment and oversight of the compliance program. Eric Newberry is

the designated Privacy Officer and all concerns or inquiries regarding FACTA should be directed to the Privacy Officer as a single point of contact to investigate and address any issues related IDT Red Flags.

1. Updates to Plan on "As Needed" Basis

The Privacy Officer is also responsible for ensuring that the program is updated whenever risks parameters change that could affect safety and soundness of the security of customer data.

2. Annual Report

The Privacy Officer will present an annual report of the Privacy Committee's activity to AUB's board of directors for review and approval. The report will include any incidents reported during the period and will outline the Privacy Committee's plans regarding necessary program revisions.

- **Designation of Privacy Committee**

As required by FACTA, AUB has appointed a Privacy committee that represents at least three critical areas that are most susceptible to identity theft and have responsibility for identifying Red Flags to help detect and mitigate IDT.

Privacy Committee Members

Member Name	Title	Key Area(s)
Chuck Forrest	IT Manager	Information Technology, Internal/External communications portals and protocols, customer database, system security
Phil Graves	Director of Management Services	Human Resources, internal personnel databases, internal medical records, payroll database information
Eric Newberry	General Manager	Executive Management, General Oversight
Michelle Millsaps	Director of Accounting	Chief Financial Officer, general accounting, plant accounting, account payments, bank draft, information technology

6.1 Privacy Committee Roles and Responsibilities

6.1.1 Needs Assessment

The Privacy Committee, in consultation with various task area employees at AUB, will complete a Needs Assessment to help the Privacy Committee identify AUB's strengths and weaknesses relative to ID Theft prevention, identification, and mitigation.
The Needs Assessment is included in this Policy and Procedure as Attachment PP AUB-05-11-A2

1. FACTA Compliance Checklist

The Privacy Committee will complete a checklist of FACT act planning/implementation activities, AUB operations relative to collection/use of sensitive customer information, IT/data security measures, and other pertinent task areas to ensure we cover all requirements and/or needs to implement and maintain a successful ID Theft Prevention, Identification and Mitigation Program.

The FACTA Compliance Checklist is included in this Policy and Procedure as Attachment PP AUB-05-11-A3

6.1.3 Develop New and Revise Existing Policies to Ensure FACTA Compliance

The Privacy Committee will write/revise policies and procedures relative to:

1. Training pertinent employees on a need-to-know basis regarding identification of Red Flags that may indicate ID theft activity.
2. Actions to be taken arising from Red Flags.
3. Preventing, Identifying and Mitigating Security Breeches
4. IT audits to monitor risks for theft
5. Reporting ID theft
6. Responding to address discrepancies

1. Training Employees Responsible for FACTA Related Information

Members of the Privacy Committee will train all pertinent employees on a need-to-know basis relative to their role in AUB's program. Refresher training will occur at least once annually.

2. Meeting of Privacy Committee

The Privacy Committee will meet at least quarterly to discuss any reported incidents or red flag occurrences and will document any AUB actions including necessary revisions to this plan or to policies/procedures.

- **Miscellaneous Administrative Policies/Procedures**

As required by FACTA, AUB has developed a number of policies/procedures related to various aspects of Red Flag identification, training and response by employees. These miscellaneous policies and procedures are listed below and included as Attachment PP

Attachment AUB PP 05-11-A1

Identity Theft Prevention Plan
Athens Utilities Board

Identity Theft Prevention Plan
Athens Utilities Board
October 2008

To comply with the Fair and Accurate Credit Transactions Act of 2005 (FACT Act), AUB's management team, privacy committee, and board of directors has generated and approved the following plan that will serve to underpin AUB's efforts to prevent, identify, and mitigate identity theft at AUB.

A. AUB has formed a Privacy Committee that includes:
   1. *Eric Newberry, General Manger*
   2. *Phil Graves, Director of Management* Services and HR representative
   3. *Michelle Millsaps, Superintendent of Accounting* and representing billing, cashiers, IT oversight
   4. *Chuck Forrest, IT Manager*

B. Members of the Privacy Committee and the Privacy Officer were appointed by the General Manager based on each person's role at AUB relative to ID Theft program needs. Members will serve indefinitely, and new members may be added as needs arise.

C. The Privacy Committee, in consultation with various task area employees at AUB, will complete a Needs Assessment to help the Privacy Committee identify AUB's strengths and weaknesses relative to ID Theft prevention, identification, and mitigation.

D. The Privacy Committee will complete a checklist of FACT act planning/implementation activities, AUB operations relative to collection/use of sensitive customer information, IT/data security measures, and other pertinent task areas to ensure we cover all requirements and/or needs to implement and maintain a successful ID Theft Prevention, Identification and Mitigation Program.

E. The Privacy Committee will write/revise policies and procedures relative to:
   1. Training pertinent employees on a need-to-know basis regarding identification of Red Flags that may indicate ID theft activity.
   2. Actions to be taken arising from Red Flags.
   3. Preventing, Identifying and Mitigating Security Breeches
   4. IT audits to monitor risks for theft
   5. Reporting ID theft
   6. Responding to address discrepancies

7. Disposal of records

F. Members of the Privacy Committee will train all pertinent employees on a need-to-know basis relative to their role in AUB's program. Refresher training will occur at least once annually.

G.

H. The Privacy Committee will meet at least quarterly to discuss any reported incidents or red flag occurrences and will document any AUB actions including necessary revisions to this plan or to policies/procedures.

I. The Privacy Officer will present an annual report of the Privacy Committee's activity to AUB's board of directors for review and approval. The report will include any incidents reported during the period and will outline the Privacy Committee's plans regarding necessary program revisions.

Attachment AUB PP 05-11-A2

Needs Assessment

Red Flag/Identity Theft Program Needs Assessment

Opening a New Account

Identify the steps in establishing service for a customer.

1. **What identification is required? How do you obtain identifying information and verify identity?** ***Gov't issued photo ID such as DL or other official ID. Signature on ID is compared to real-time signature on AUB application. If no match, we may ask for SSN to check historical accts to see if customer has a poor history with AUB and is attempting to sign up with someone else's ID to get service and avoid paying off old debt.***
2. **Do they need to make the application in person or can they send in the information in an alternate form? Telephone or other?** ***We allow for faxed application and IDs, but require that they ultimately come by the office to actually sign the application.***
3. **Does the utility use consumer reports in the application process? How? Establish deposit? Approve or deny services?** ***No.***
4. **Does the utility have policies and procedures that define red flags for identity theft and actions for mitigation?** ***Not currently; now in development for FACTA compliance.***
5. **What happens to the hand written notes made by the CSR in the application process?** ***Notes are filed monthly in bankers boxes in storage and are eventually destroyed.***
6. **Is the computer screen visible to others during the application process? No.**
7. **Who has access to data once entered? Does the CSR lock computer when not at desk?** ***Most all employees with workstations have limited access to utility billing information in our CIS; however, sensitive information is limited to need-to-know employees by the IT administrator. Currently, CSRs do not lock their workstations when not at desk. Will be a new procedure.***
8. **If applicant gives address, bank account, date of birth or social security number verbally to CSR, what precautions are taken from others hearing?** ***CSRs do not take bank info, and we no longer collect SSNs. If one is needed, the customer is asked to write it down and show it to the CSR rather than broadcast it.***
9. **Once personal identification information is entered by CSR, where and how can it later be retrieved?** ***Using CIS or Milner***
10. **What safeguards are currently built into the application process?** ***We no longer collect sensitive info in the app process. Signatures on apps are compared with those on official IDs.***
11. **What safeguards would you like to implement?** ***Remove SS# from CIS and Milner***
12. **Which employees have access to information – is it on a "need to know" basis?** ***CSRs. Billing, cashiers, Yes, NTK basis managed by the IT administrator***
13. **Is any customer personal information carried into the field on a laptop?** ***No, sensitive info is stripped before any GIS computer is populated***

Customer Initial Contact

-Customer requests service either in person or, if applicant is out of state, by phone via AUB customer service.

-CSR has applicant sign an AUB service application card and attaches to the application a photocopy of a driver's license or other official government-issued ID. If application is by phone CSR and applicant exchange fax versions of application and ID.

-CSR initiates a service order to have the requested service established.

-Service order is processed through AUB such that account is routed (if need be) and added to the billing system.

-Service is established.

Needs Assessment continued

Monitoring an Existing Account

Identify the possible red flags that may exist in the following procedures:

- Authenticating transactions for existing customers
- Monitoring activity/transaction of customers
- 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?

Does your utility use passwords or some form of security access?

Passwords are used and a forced change every 4 months is in place

Describe your process for verifying/validating the following:

Check by phone_____

Credit Card Number: See "Credit Card and Bank Draft Procedures" document in FACTA files

Are receipts ever printed? If so, what part of number is exposed? See above on CC procedures

In what manner have customers attempted to fraudulently represent themselves as someone else in a transaction in an existing account? Customers have, on occasion, tried to negate a cutoff by saying that they were not the person who signed for the account originally. We have not had an instance where a misrepresentation was aimed at ID theft, only at an attempt to maintain service.

What safeguards are currently built into monitoring existing utility accounts?

Only certain AUB employees can access certain areas of the CIS.

What safeguards would you like to implement? TBD

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

How do you authenticate transactions for existing accounts?

Request

-Electronic or physical access to account information is limited only to certain AUB employees, which in turn have access only to the screens that are necessary for their job function. Non-employees do not have such access.

-We do not store sensitive information on the CIS. If a request for account info comes from the public, no information is given out other than information deemed "public" under current law.

-If a request comes in by phone to alter the status of an account, such as to discontinue services, the CSR asks for verification of the ID number associated with the account, such as driver's license number.

After you have mapped out the flow of information, identify possible areas where the protection of secured information could be improved.

Attachment AUB PP 05-11-A3

Compliance Checklist

Compliance Checklist

Identity Theft Prevention Program Red Flags Implementation Checklist for Utilities

Privacy Officer: Eric Newberry

Committee Members: Michelle Millsaps
Phil Graves
Chuck Forest

Question	Comment			Yes/No Date
Has a privacy officer and committee been established?				Yes 8/18/08
Does the committee have representations from at least 3 key areas?				Yes
Are defined responsibilities outlined for committee members?				Yes
Is there a written identity theft prevention plan?				Yes
Does the written plan provide a policy/procedure for:				Yes
1. Preventing/Identifying and Mitigating Red Flags				Yes
2. Handling a breech in security				Yes

Question	Comment			Yes/No Date
3. Record Disposal				Yes
4. Customer Request Records				Yes
5. IT security internal				Yes
6. IT security external				Yes
7. Screening/Hiring and Training Key Employees handling sensitive information				Yes
8. Privacy Officer/ Committee Members roles/ terms of service/ method for appointment	*See AUB ID Theft Prevention Plan*			Yes
9. Program assessment and revision	*See ID Theft Prevention Plant*			Yes
10. Program reports tracking incidents & resolutions - Report to General Manager and Board of Directors	*See ID Theft Prevention Plant*			Yes
Utility has requested from local identity theft police officer/detective: Reporting procedures and document training	*Name of Contact: Chief of Police Contact Info: Athens Police Dept.*			Yes

Question	Comment			Yes/No Date
All current employees involved in handling sensitive information have received identity theft prevention training/red flags	Names of Employees See electronic FACTA file "Employee Training sign-up sheet"	Date Trained Oct. 8 and 9, 2008 Thereafter, annually each fall.	Trainer Eric Newberry, AUB compliance officer	Yes
Human Resources has incorporated the identity theft prevention skills in the: orientation and performance evaluation of key positions	HR manager will incorporate an ID theft sign off as part of the orientation that includes sign off on the employee handbook. This will apply only to the need-to-know positions that are trained in our ID theft prevention system: Accounting, Data Processing/IT, Customer Service, Cashiers, HR			
IDTPP updates are provided on a continual basis to key employees: trends in theft, legislation, IT as well as best practices/mitigation procedures				Ongoing
Procedures for employees as they leave the utility	*User account is removed*			Yes
Consultants sign written 3rd party contracts which outline the consequences of breaking security regulations	*To Be Determined*			**No**
Are there any routines for the end of assignments	*Clean IT system to remove the consultant's authority*			Yes
Information Classification				NA

Question	Comment	Yes/No Date
Is there a system for information classification according to the appropriate level of availability? (e.g. open, confidential, secret)		
Does the classification system require encryption for any class or type of information?		NA
Is there a classification checklist to make it easy for the user to determine information class?		NA
Software Are there any instructions for bringing outside software/data into the utility?	*Software installation is limited* *See AUB Computer Use Policy (CUP)*	Yes
Are policy documents and security guidelines considered during developing systems?	*Security features must be implemented from the beginning.*	NA
Are security requirements included in the demand specification when buying or developing systems?	*The requirements must be included from the beginning.*	Yes
Are system tests and development separated from production systems?	*Avoid compilers and editors in production systems. (More vulnerable to hackers if able to compile in production)*	NA
Are security-related patches from developers and/or vendors implemented as soon as possible?	*Routine will include a download to a test environment.*	Yes
Is a security validation approval done before introducing new software? Individual users should not be allowed to introduce new software.	*New software might create new holes in the system. For example employee may download a game which contains a keystroke logger. Information is sent to the hacker. Install rights limited*	Yes
Is there a routine for installing a new operating system?	*This is the most critical software and all configuration parameters must be checked before rebooting.*	Yes
Is it a classified operating	*According to ITSEC, TCSEC, Common*	Yes

Question	Comment	Yes/No Date
system?	*Criteria*	
Are security options in the operating system activated?	*Passwords changed every 120 days*	Yes
Are there any routines to change all security related default parameters in the operating system?	*Security is determined by server when computer joins the network*	Yes

Question	Comment	Yes/No Date
Are there any routines to request all patches that are needed to preserve the security?	*To prevent hacking possibilities. Patched applied as applicable (Note Patch = Repair to Program)*	Yes
Are 'system-tools' protected?	*Software to administer and service the system. Password protected*	Yes
Are the use of 'system tools' restricted to just a few persons?	*Administrators*	Yes
Is all use of 'system-tools' logged?	*Not all tools have a log function*	No
Is anti-virus software installed and activated?	*Updated automatically*	Yes
Do the users know how to handle viruses?	*Deleted or quarantined automatically*	Yes
Are there any extended controls of software downloaded from WAN such as Internet?	*Software downloads are limited by the firewall and AUB CUP*	Yes
Are the users informed about software licenses, as to what extent they are allowed to copy them and use them in other equipment? If they are allowed to use them for private use at home, etc.?	*Users do not have access nor are they allowed to take software for home use per CUP*	Yes
Is loading of new software regulated?	*Most users do not have access*	Yes
Is critical software backed up and stored in another safe place?	*Disk to disk, disk to tape and offsite*	Yes
Is critical software protected by checksums?		Yes
Is all software from well-known sources?	*Special notice on encryption software.*	Yes
Hardware	*See AUB Computer Use Policy*	Yes
Are there any instructions for bringing equipment outside the organization?		
Are there instructions on how to discard equipment?	*IT Administrator discards*	Yes
Is it made clear that the equipment is for business use	*See AUB Computer Use Policy*	Yes

Question	Comment	Yes/No Date
only and not for private use by the user?		
Are policy documents and security guidelines considered during introduction of new equipment?		Yes
Are security requirements included in the demand specification when buying or changing equipment?	*The requirements must be included from the beginning.*	Yes
Is a security validation made before introducing new hardware?	*New hardware might create new holes in the system.*	Yes
Is there a person responsible for each workstation/personal computer?	*Admins*	Yes
Do the laptops used for field work-mapping software-also contain customer personal ID info? How is ID protected?	*Information is stripped before data population* *Boot password and logon password*	Yes
Documentation		
Is the management policy document printed and distributed to all members of staff and subsequently to new members?		
Is there an Information Security handbook?	*None*	No
Are systems and manual routines well documented?	*To prevent the sole dependence on key-persons. Some have documentation*	Yes
Are there documents describing: A. Hardware B. Software C. Applications D. Communication Are they up to date?		No

Question	Comment	Yes/No Date
Do handbooks for each staff category exist? A. Developer B. Administrators (network, database etc.) C. Users D. Helpdesk E. Etc.		No
Are there written rules defining responsibility and authority for each staff category?	*Job description*	Yes
Are system documents stored in a safe place?		Yes
Do security logs track log ins, users and application?	*Login*	Some
Computer Media Are there any routines for labeling media?	*Date*	Yes
Is the existence of media checked on a regular base?	*Media in the inventory list.*	Yes
Are there any routines to handle missing media?		No
Are there any routines for archiving media?	*Back up servers on nightly basis and archive.*	Yes
Are there any routines for transporting and storing media?		No
Are there any routines for destroying media?	*Degauss tape* *Break CDs*	No
Are there any routines for how to handle media during service?	*Don't leave media unattended during service and don't let media with sensitive information leave your organization.*	Yes
Identification and Authorization		
Does the system include logging and alarm functions? For example is someone attempts to log in 3 times unsuccessfully, is a message sent to the network administrator?	*Logins are monitored and the system will lock after 5 attempts*	Yes

Question	Comment	Yes/No Date
Does the system include access control to resources/objects?	*Password*	Yes
Is it quality tested on password/PIN?	*Password must meet complexity requirements*	Yes
Is it possible to reuse old passwords/PIN?	*4 previous are remembered and not allowed*	Yes
Is it possible to use the user ID as password/PIN?		No
Are there any routines to change software default passwords?	*Upon installation, is the software default password changed?*	Yes
Is the number of log in attempts limited?		Yes
Is the change of password/PIN compulsory after a certain number of days?	*120*	Yes
Does the system block an account if the password is not changed within the time limit or the account has been remained unused?		Yes
Is it possible for a user to change their privileges?		No
Is the password/PIN encrypted? (one way encryption)	*Hashed*	Yes
Is the password/PIN individual?	*Must be.*	Yes
System Security	*Systems use network time servers*	Yes
Is there a routine to ensure the correct date and time in all systems and are they synchronized?		
Are there enhanced logging facilities in critical systems?	*None*	No
Are there documented procedures for changing the network?	*Only the IT manager and direct backup have electronic authority to make such changes.*	Yes
Are all changes to the network documented?	*Not currently*	No
Are open ports on HUB blocked?	*Physical access*	Yes

Question	Comment	Yes/No Date
Is the network administrator privilege restricted to a few users?	*Admin*	Yes
Is all network hardware (HUB, Repeaters, Routers, Gateways, etc.) well protected?	*Physical and password*	Yes
Is the software in the network hardware well protected? Use strong authentication for changing the software or configuration.		Yes
Internal Protection Is an IDS (Intrusion Detection System) installed?	*Inside firewall*	Yes
Protection from Outside Sources Is a firewall installed?		Yes
Is there a routine for the administration of the firewall?	*Firewalls are set up and continually updated by IT personnel.*	Yes
Is the use of encryption considered?	*Is there a trustworthy algorithm and key administration?*	Yes
Is access to communication ports for service protected?	*Physical*	Yes
Are VPN (Virtual Private Networks) used?		Yes
Logging		
Are the log files protected against unauthorized access?		Yes
Is the system configured in a way that the log must be turned on?		Yes
What events are logged: A. Login B. Logout C. Failed login D. Exceptional behavior E. Access violation Activities in the Identification and Authorization system?		Yes
Physical Protection		Yes

Question	Comment	Yes/No Date
Are all premises protected?		
Are computers and network components placed in an access protected area?		Yes
Is all system documentation safeguarded?		Yes
Are communication lines protected?		Yes
Is there an admission and leaving control system with a log?		Yes
Server room is under lock and key.		Yes
Is there an up to date list with authorized people?		No
Incident handling		No
Is there a plan for how to handle incidents?		
Contingency planning	*Disaster recovery site*	Yes
Is there a contingency plan? How to recover the system after an incident?		

Attachment AUB PP 05-11-A4

Miscellaneous Policies and Procedures Relating to FACTA

A - Employee Training

B - Defining Actions from Red Flag Identification

C - Preventing, Detecting, and Mitigating Security Breeches

D - Disposal of Records

E - IT Audits to Monitor Risk

F - Response to Address Discrepancies

G - Request for Customer Account Information

H - Reporting ID Theft

A - Providing Designated Employees with Identity Theft Prevention Training

1. Designated employees will be trained on a need to know basis according to job responsibilities.
2**. Initial Training** is provided on three levels:
A) The **Privacy Officer** attended a 1.5 day seminar regarding FACTA compliance.
B) **Privacy Committee members** participated in a two-hour work session on Identity Theft Prevention Program covering principles of needs assessment, program design, development, implementation and evaluation. Strategies for revision and reporting were included.
C**) Employees** will be trained on a need to know basis in an initial session of approximately two hours. Training will include and may not be limited to: a recap of the overall program and the utilities role; lessons in identifying and reacting to red flags; prudent steps to take to protect sensitive data; steps for reporting ID theft; ID theft vs. fraud; document disposal
3. **Annual Updates** will be provided for all designated employees. Sessions to be a minimum of 30 minutes will include, but not limited to the same topics as in initial training, plus possible recaps of the Privacy Committee's activities on a need to know bases.
4. **Documentation of Training**
A) Training will be documented by the secretary for the Privacy Committee in the same way committee meetings are documented with minutes. For training, an agenda of the session will be included in the documentation. The agenda and minutes will be filed in the Privacy Officer's electronic FACTA files.
5. New employees hired into positions handling secured information will receive initial training within 30 days of employment.

B - Defining Action(s) to be taken for each of the Red Flags that relate to the opening of new accounts and the monitoring to existing accounts.

Procedure:

AUB has identified the following steps to help detect, prevent and mitigate identity theft in connection with establishing accounts or servicing existing accounts.

AUB submits the follow actions relative to Red Flags. Responses may include but may not be limited to actions in the following table.

Flag	Next Step	Mitigation **(Steps to Control Losses)**
Alerts		
Consumer report indicates fraud or active duty alert.	**CSR notes the alert to the applicant and attempts to call the applicant via the phone number he/she provided to the CRA when requesting the alert be placed on the file.**	**If alert contact info on file with the CRA does not allow contact with the AUB applicant, CSR explains that no account can be opened until the applicant takes necessary steps with the CRA regarding contact information for creditors.**
Credit freeze.	**CSR informs applicant of the current freeze on the consumer's credit information.**	**AUB will not open an account for the subject applicant until he/she has taken appropriate steps with the CRA to lift the freeze on the report.**
Notice of address discrepancy from CRA.	**If applicant is unknown to AUB, CSR will work to obtain identification from the applicant that provides a reasonable certainty as to the applicant's identity and validity of the new address.**	**CSR reports new address, once AUB is confident, to the CRA for the purpose of records updating.**
Unusual patterns in activity.	**CSR notifies applicant of alert regarding activity.**	**If applicant is unaware of the reported activity, CSR will work with the customer at his/her will to contact the CRA so that the applicant can obtain further information.**
Presentation of Suspicious Documents		
Identification documents appear altered or forged.	**CSR explains to applicant that we cannot establish an account using such apparently altered/forged documents. Requests customer to return after obtaining proper documentation.**	**If subject document is an official government issued ID, such as DL, AUB may contact local law enforcement to alert them to the situation.** **If subject document is a "lower level" document such as a lease agreement or rent receipt, CSR may contact the landlord to discuss/verify the situation.**

Flag	Next Step	Mitigation **(Steps to Control Losses)**
Photo/physical description does not match applicant.	**CSR explains that a new account cannot be opened using the subject form of ID. Requests prospect to return at later time with proper ID.**	**If subject document is an official government issued ID, such as DL, AUB may contact local law enforcement to alert them to the situation.**
Other information on identification is inconsistent information given from applicant.	**CSR may raise issue to supervisor level. If the inconsistency is material in nature, AUB may reject application pending receipt of proper ID.**	**If subject document is an official government issued ID, such as DL, AUB may contact local law enforcement to alert them to the situation.**
Information in utility files in inconsistent with information provided. Example – signatures do not match on signature card.	**This type issue occurs most often regarding very old AUB information, such as old signature card that predates AUBs use of gov't ID when establishing account. Works through the issue with prospect to determine reason for inconsistency.**	**Ensure that any new account is established using current proper ID. If transaction raises level of suspicion to the point where ID theft is suspected, AUB may contact local law authorities with information.**
Application looks altered or forged or destroyed and reassembled.	**Applications are not brought in from outside, but are filled out in AUB offices.**	**NA**
Suspicious Personal Identifying Information		
Identification is inconsistent with external source such as: A. Address v. Address on Consumer Report B. Social security number not issued. C. Social security number on Death Master file.	**CSR informs applicant of any discrepancies and works to gain a reasonable assurance of the applicant's identity by use of alternative means, such as other forms of official ID.**	**If applicable, CSR aids applicant in contacting local SSN administration office.**

Flag	Next Step	Mitigation **(Steps to Control Losses)**
D. Inconsistent information, such as lack of correlation between date of birth and social security number.		
Identification is known to be associated with fraudulent activity: A. The address is fictitious, a prison or a mail drop on application. B. The phone number is invalid or associated with a pager or answering service. C. The social security number is the same as that submitted by other persons opening an account. D. The address is the same address as that submitted by other persons opening an account.	**If ID is <u>known</u> to be associated with fraud, AUB may contact local law enforcement.**	**AUB may notify a current customer if an applicant comes in with fraudulent info pertaining to the current customer's account, and would recommend that the customer then start the process of notifying law enforcement and other pertinent entities such as their CC companies, etc.**
Applicant fails to provide all personal ID requested.	**CSR informs applicant that service cannot be established until required ID is presented.**	**No acct opened until ID submitted.**
Personal ID is inconsistent with utility records.	**AUB will initially work with applicant to understand reason for discrepancy. If fraud/theft is suspected, AUB may take mitigations steps.**	**AUB may contact local law enforcement if discrepancy indicates that ID fraud/theft is a possible motive.**
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.	**AUB does not use challenge questions because we do not give out sensitive information over the phone, only public information.**	**NA**
Change of billing address is followed by request for adding additional properties	**CSR notifies customer that additional properties cannot be**	

Flag	Next Step	Mitigation **(Steps to Control Losses)**
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).	**added to an additional account; new properties would require new accounts that must past scrutiny like any other. Further, to add any new names as account holders, the new holders must come to AUB and fill out application paperwork including DL info, etc.**	
Payments are made in a manner associated with fraud. For example, deposit or initial payment is made and no payments are made thereafter.	**In this case, account would be terminated.**	**Initial applicant would not be able to open new AUB accounts without clearing old account and without using legitimate supporting ID documentation.**
Existing account with a stable history shows irregularities.	**If this condition came to our attention, CSR may contact customer to gain understanding of issues.**	
Mail sent to customer is repeatedly returned.	**CSR may request service to attempt to verify whether location is still occupied. CSR may attempt to contact customer.**	**Account will be terminated if billings are returned unpaid.**
Customer notifies utility that they are not receiving their bill.	**CSR verifies mailing address. If same, CSR recommends customer contact USPS and to consider beginning ID theft/fraud steps.**	
The utility is notified of unauthorized charges or transactions in connection with a customer's account.	**NA to our operations.**	
Notice of Theft		
Utility is notified by law officials or others, that it has	**Cooperate with law**	

Flag	Next Step	Mitigation **(Steps to Control Losses)**
opened a fraudulent account for a person engaged in identity theft.	**enforcements wishes.**	

C - Preventing, Detecting and Mitigating Breaches in Security

• In the event of a breach of security involving sensitive customer information, the following precautions will be taken to mitigate damage: 1. Disconnect external connections. 2. Revoke /change access passwords. 3. Evaluate risk associated with breach. 4. Check for data integrity. 5. Load archive copy of firewall settings.
• Notification within the utility will follow: The IT manager will notify his direct supervisor (AUB's Accounting Superintendent), the company Privacy Officer, and the General Manager.
• Customers whose accounts are known to be affected by the breach will be contacted by the best available communications method to ensure timely contact, such as by phone if the number is available or USPS by using the current billing address. These customer contacts will begin with 48 hours of verification of any breach.

D - Disposing of Records

- AUB contracts with an outside vendor, Shred It, Inc., to dispose of all sensitive printed or written documentation. Locked receptacles have been placed in designated locations within the AUB offices near work areas where such information may be generated or stored, such as the customer service area and the billing/data processing area. The vendor picks up and shreds once-a-month. A certificate of shred is provided by the vendor upon request by AUB.
- Some records may be stored for reference rather than placed in the locked receptacles. For such records, AUB has records retention schedules and policies.

E - Conducting IT Audits to Monitor Risk for Identity Theft

1. AUB will utilize the Identity Theft Prevention Program Checklist to audit and evaluate internal and external identity theft risk in information technology security.

1. AUB will conduct walk through inspections every 4 months by the AUB IT Manager and his assistant and complete audits will be completed on a yearly basis by these same IT personnel.

   The IT Manager will conduct the following checks:

   Passwords are changed regularly
   Physical assets are secure and accounted for
   Data backlogs and restores are tested
   Access logging is functional
   Virus and spam filters are updated
   Train and warn employees regarding spam, phishing, and other threats as well as password training.

3. Recommendations to reduce risk of identity theft will be submitted for program review and evaluation upon completion of an audit checklist. Results will be submitted to the privacy officer 2 weeks of completion of the evaluation.

F - Responding to Notices of Address Discrepancies

1. AUB will furnish a confirmed address to a consumer reporting agency (CRA) under the following conditions:

e. Utility has established relationship with the CRA. Currently AUB does not use any CRA.

b. Utility can form a reasonable belief the consumer report relates to the consumer

about whom the user request the report.
c. The consumer under review is a current customer with an active account.
d. Request involves a customer opening a new account.
e. CRA provides request (*state your terms- in writing-time period*)

G - Responding to Requests for Customer Account Information

1. AUB will furnish publically available information from utility accounts under the following conditions:
a. That the information requested is deemed public information pursuant to applicable federal and state law and in no way includes sensitive financial or identifying information, such as bank numbers, CC numbers, SSNs, gate codes, alarm codes, etc.
b. That the requested information is in no way subject to an Order of Protection and is not part of a formally established Protection Document File.
c. That the requested information is not relative to the location of a Protected establishment such as a Domestic Violence Shelter or Rape Crisis Center.

H -Handling Reports of Suspected Identity Theft

1. When a consumer suspects identity theft, he must notify the utility in writing, completing the Federal Trade Commission Affidavit. Instructions for completion are included as part of the form.
2. Customer will be asked to submit a copy of affidavit with police report to AUB's Privacy Officer.
3. Privacy Officer or designee will make a copy of the customer's photo ID.
4. Privacy Officer or designee will record the receipt of documents.
5. Privacy Officer or designee will, in cooperation with the customer, submit the copies of the FTC affidavit, police report and photo ID to local law enforcement.
6. Pertinent AUB personnel may go over the customer's account with the customer to verify all information and activity as legitimate and will change/purge information as necessary in conjunction with information provided by the customer, such as change in credit card information, etc.