RESOLUTION NO. 784

A RESOLUTION OF THE MEMBERS OF CLINTON CITY COUNCIL ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM; APPOINTING AN OVERSIGHT COMMITTEE; AND AUTHORIZING THE CITY MANAGER TO APPROVE MODIFICATIONS TO THE PROGRAM AS NEEDED

WHEREAS, pursuant to federal law the Federal Trade Commission adopted Identity Theft Rules requiring the creation of certain policies relating to the use of consumer reports, address discrepancy and the detection, prevention and mitigation of identity theft;

WHEREAS, the Federal Trade Commission regulations, adopted as 16 CFR § 681.2 require creditors, as defined by 15 U.S.C. § 1681a(r)(5) to adopt red flag policies to prevent and mitigate identity theft with respect to covered accounts;

WHEREAS 15 U.S.C. § 1681a(r)(5) cites 15 U.S.C. § 1691a, which defines a creditor as a person that extends, renews or continues credit, and defines 'credit' in part as the right to purchase property or services and defer payment therefore;

WHEREAS the Federal Trade Commission regulations include utility companies in the definition of creditor;

WHEREAS the City of Clinton, Oklahoma is a creditor with respect to 16 CFR § 681.2 by virtue of providing water, sewer and sanitation utility services;

NOW, THEREFORE, BE IT RESOLVED BY THE MEMBERS OF CLINTON CITY COUNCIL :

Section 1. The Council hereby adopts an Identity Theft Prevention Program in accordance with the requirements of the Fair and Accurate Credit Transaction Act.

Section 2. The Council appoints the City Manager as the Oversight Committee to oversee the operation and compliance of the Authority's Identity Theft Prevention Program.

Section 3. The Council authorizes the City Manager to approve modifications to the Identity Theft Prevention Program as needed to meet the needs of the utility department and to maintain compliance with the Fair and Accurate Credit Transaction Act.

PASSED AND APPROVED THIS _____ DAY OF _____, 2009.

CLINTON CITY COUNCIL

By:_____
Mayor

ATTEST:

_____
Secretary

(SEAL)

CITY OF CLINTON
IDENTITY THEFT PREVENTION PROGRAM

PURPOSE OF PROGRAM

Pursuant to federal law the Federal Trade Commission adopted Identity Theft Rules requiring the creation of certain policies relating to the use of consumer reports, address discrepancy and the detection, prevention and mitigation of identity theft. The Federal Trade Commission regulations adopted as 16 CFR § 681.2 require creditors, as defined by 15 U.S.C. § 681(a)(5) to adopt red flag policies to prevent and mitigate identity theft with respect to covered accounts. 15 U.S.C. § 1681a(r)(5) cites 15 U.S.C. § 1691a, which defines a creditor as a person that extends, renews or continues credit, and defines "credit" in part as the right to purchase property or services and defer payment therefore. The Federal Trade Commission regulations include utility companies in the definition of creditor. City of Clinton ("COC") is a creditor with respect to 16 CFR § 681.2 by virtue of providing utility services or by otherwise accepting payment for municipal services in arrears.

The Federal Trade Commission regulations define "covered account" in part as an account that a creditor provides for personal, family or household purposes that is designed to allow multiple payments or transactions and specifies that a utility account is a covered account. The Federal Trade Commission regulations require each creditor to adopt an Identity Theft Prevention Program which will use red flags to detect, prevent and mitigate identity theft related to information used in covered accounts. COC provides water, sewer, and sanitation services for which payment is made after the product is consumed or the service has otherwise been provided which by virtue of being utility accounts are covered accounts. COC residential customer accounts for water, sewer, and sanitation services for which payment is made after the product is consumed or the service has otherwise been provided are covered accounts by virtue of being for household purposes and allowing for multiple payments or transactions.

The Federal Trade Commission regulations adopted as 16 CFR 681.2, require users of consumer credit reports to develop policies and procedures relating to address discrepancies between information provided by the consumer and information provided by a consumer credit company. COC does not now use consumer credit reports to establish various customer accounts, but may at some time in the future begin using consumer credit reports. Accordingly, COC has enacted this Identity Theft Prevention Program in compliance with federal law.

1. Purpose.

The purpose of this Program is to comply with 16 CFR § 681.2 in order to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will prevent identity theft.

2. Definitions.

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

(a) "COC" means the City of Clinton.

(b) "Covered Account" means (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; (ii) Any other account that the financial institution or creditor offers or maintains or which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(c) "Credit" means the right granted by the creditor to a debtor to defer payment of debt to incur debts and defer its payment or to purchase property or services and defer payment therefore.

(d) "Creditor' means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.

(e) "Customer" means a person that has a covered account with a creditor.

(f) "Customer Service Representative" (CSR) means an individual working for COC whose principal responsibilities include attending to customers and their needs.

(g) "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any,

(1) Name, social security number, date of birth, official State or government issued driver's license, alien registration number, government passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address or routing code; or

(4) Telecommunication identifying information or access device.

(h) "Identity theft" means a fraud committed or attempted using identifying information of another person without authority.

(i) "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

(j) "Notice of address discrepancy" means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. § 1681(c)(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(k) "Oversight Committee" means the Committee appointed by COC to oversee operation and compliance of the COC ITPP in accordance with the requirements of the Fair and Accurate Credit Transaction Act.

(l) "Personal Identifying Information" means a person's credit card account information, debit card account information bank account information and drivers' license information and for a natural person includes their social security number, mother's birth name, and date of birth.

(m) "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(n) "Service provider" means a person that provides a service directly to COC.

3. Findings

(1) COC is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is make in arrears.

(2) Covered accounts offered to customers for the provision of COC services include residential water, sewer, solid waste, building permits, business licenses, facility rentals, legal fees and fines, and other misc. fee, permits and licenses.(3) COC has no known prior experience with identity theft related to covered accounts.

(4) The processes of opening a new covered account, restoring an existing covered account, making payments on such accounts, and transferring such accounts have been identified as potential processes in which identity theft could occur.

(5) COC limits access to personal identifying information to those employees of the City of Clinton who are responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for use of a covered account. All written applications associated with the covered accounts are maintained in areas of minimal access: (ie: vault or locked file cabinets). Information provided in the applications is entered directly into COC's computer system and is accessible only to those employees whom have been designated by the City Manager and to COC's computer technician.

(6) COC has determined that there is a low risk of identity theft occurring in the following ways, if any:

a. Use by an applicant of another person's personal identifying information to establish a new covered account;
b. Use of a previous customer's personal identifying information by another person in an effort to have service restored in the previous customer's name;
c. Use of another person's credit card, bank account, or other method of payment by a customer to pay such customer's covered account or accounts;
d. Use by a customer desiring to restore such customer's covered account of another person's credit card, bank account, or other method of payment; and
e. Use by a third party of a customer's personal identifying information obtained by overhearing conversations between COC and the customer during the customer's application for service process.

4. Process of Establishing a Covered Account.

(1) As a precondition to opening a covered account in the COC, each applicant shall provide COC with personal identifying information of the customer which shall be in the form of one (1) of the following from Group A: A U.S. Government issued passport,(expired or unexpired), Certificate of U.S. Citizenship, Certificate of Naturalization, Unexpired Foreign Passport, Permanent Resident Card or Alien Registration Receipt Card with Photo, or an unexpired Employment Authorization Document that contains a photo; or two (2) forms of the following: one (1) from each group: Group B: Photo Driver's License, Photo ID Card issued by a state or outlaying possession of the United States, Photo ID Card issued by the Federal, State, or Local Government Agencies, School ID with Photo, Voter's Registration Card, U.S. Military Card, Draft Record, or Military Dependent's ID Card; Group C: U.S. Social Security Card, Certificate of Birth Abroad issued by the Department of State, Original or Certified Copy of Birth Certificate issued by State, County, Municipal Authority bearing an official U.S. Seal, Native American Tribal Document or U.S. Citizen ID Card. For customers who are not natural persons such as a trust, the customer's agent opening the account must provide a valid State or Federal Government issued Identification Card and proof of authority to act on behalf of the trust.

If an applicant's name has been changed through marriage, divorce, legal name change, or otherwise, verification of the name change must be provided before an applicant will be allowed to establish a new account or transfer an existing account in a name different from that appearing on the required State or Federal Government issued Identification Card.

(2) COC does not now use consumer credit reports. Should COC begin using consumer credit reports, each applicant shall also be required to provide any information necessary for COC to access the applicant's consumer credit report.

(3) An applicant's personal identifying information shall be entered directly into COC's computer system and all written applications shall be placed in the vault or locked file cabinets.

(4) COC employees responsible for opening new accounts shall take reasonable precautions to insure that third parties are not attempting to view personal identifying information on a written application as it is being completed by the applicant.

(5) COC does not now allow customers to pay billing statements online. Should COC begin allowing online payments, each account shall be assigned an account number and personal identification number (PIN) which shall be unique to that account. COC may utilize computer software to randomly generate assigned PIN's and to encrypt account numbers and PINs.

5. Access to Covered Account Information.

(1) Access to customer accounts shall be password protected and shall be limited to authorized COC personnel.

(2) Passwords shall be changed by the COC computer technician at the direction of the City Manager on a regular basis. The passwords shall be at least 8 characters in length and shall contain letters, numbers, and symbols.

(3) Any unauthorized access to or other breach of customer accounts is to be reported immediately to the City Manager and the password shall be changed immediately.

(4) Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the City Manager and the City Attorney.

6. Credit Card Payments.

(1) At the present time COC does not allow payments through the internet. If in the future such payments are allowed, and are processed through a third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place that is applicable to such payments.

(2) Credit card payments are not allowed by telephone or through a COC website. If in the future such payments are authorized, all credit card payments made over the telephone or COC's website shall be entered directly into the customer's account information in the computer data base.

(3) Account statements and receipts for a covered account shall include only the last four digits of the credit or debit card or the bank account used for payment of the covered account.

(4) COC employees shall not accept a credit card payment from anyone other than the person named on the credit card. If a third party's credit card is to be used to pay the account of a customer, the third party named on the credit card must present the card for payment of the customer's account and must provide verification that he or she is the person named on the credit card.

7. Sources and Types of Red Flags

All employees responsible for or involved in the process of opening a covered account, restoring a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft and such red flags may include:

(1) *Alerts from consumer reporting agencies, fraud detection agencies or service providers* (if a consumer credit report is used).

Examples of alerts include but are not limited to:

a. A fraud or active duty alert that is included with a consumer report;
b. A notice of credit freeze in response to a request for a consumer report;
c. A notice of address discrepancy provided by a consumer reporting agency;
d. Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    i. A recent and significant increase in the volume of inquires;
    ii. An unusual number of recently established credit relationships;
    iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
    iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

(2) *Suspicious documents.*

Examples of suspicious documents include:

a. Documents provided for identification that appear to be altered or forged;
b. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
c. Identification on which the information is inconsistent with the information provided by the applicant or customer;
d. Identification on which the information inconsistent with readily accessible information that is on file with COC;
e. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

(3) *Suspicious personal identification, such as a suspicious address change.*

Examples of suspicious identifying information include:

a. Personal identifying information that is inconsistent with external information sources used by COC. For example:
    i. The address does not match any address in the consumer report (if used by COC); or
    ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File (if used by COC).
b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the social security number range and date of birth.
c. Personal identifying information or a phone number or address, is associated with known fraudulent application or activities as indicated by internal or third-party sources used by COC.
d. Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.
e. The social security number provided is the same as the submitted by other applicants or customers.
f. 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 applicants or customers.
g. The applicant or customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
h. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.
    i. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

(4) *Unusual use of or suspicious activity relating to a covered account.*

Examples of suspicious activity include:

a. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    i. Nonpayment when there is no history of late or missed payments;
    ii. A material change in the water usage.

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

c. COC is notified that the customer is not receiving paper account statements.

d. COC is notified of unauthorized charges or transactions in connection with a customer's account.

e. COC is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.

(5) *Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.*

8. Prevention and Mitigation of Identity Theft.

(1) In the event that any COC employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the City Manager. If, the employee in his or her discretion deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the City Manager, who may in his or her discretion determine that no further action is necessary. If the City Manager in his or her discretion determines that further action is necessary, a COC employee shall perform one or more of the following responses, as determined to be appropriate by the City Manager:

a. Contact the customer;

b. Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's covered account:

i. change any account numbers, passwords, security codes, or other security devices that permit access to an account; or
ii. Close the account;

c. Cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;

d. Notify a debt collector within two (2) business days of the discovery of likely or probable identity theft relating to a customer account that has been sold to such debt collector in the event that a customer account that has been sold to such debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;

e. Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or

f. Take other appropriate action to prevent or mitigate identity theft.

(2) In the event that any COC employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect an application for a new account, such employee shall use his or her discretion to determine whether

such red flag or combination of red flags suggests that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the City Manager. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the City Manager, who may in his or her discretion determine that no further action is necessary. If the City Manager in his or her discretion determines that further action is necessary, a COC employee shall perform one or more of the following responses, as determined to be appropriate by the City Manager:

a. Request additional identifying information from the applicant;
b. Deny the application for the new account;
c. Notify law enforcement of possible identity theft; or
d. Take other appropriate action to prevent or mitigate identity theft.

9. Updating the Program.

The City of Clinton Oversight Committee shall annually review and, as deemed necessary by the Committee, update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of COC and its covered accounts from identity theft. In doing so, the Committee shall consider the following factors and exercise its discretion in amending the program:

(1) COC's experiences with identity theft;
(2) Updates in methods of identity theft;
(3) Updates in customary methods used to detect, prevent, and mitigate identity theft;
(4) Updates in the types of accounts that COC offers or maintains; and
(5) Updates in service provider arrangements.

10. Program Administration.

(1) In accordance with specified guidelines, the COC governing board has designated an Oversight Committee composed of the City Manager and those appointed by him/her to ensure the Program's regulatory compliance. The Oversight Committee is responsible for, but not limited to,

- The development and implementation of the Program;
- Approval of the written Program;
- Ensuring compliance with all Program requirements as stated in this policy; and,
- Conduct a periodic review of all incidents involving one or more red flag events every six months (on or about May 1 and November 1 of each year).
- At least annually, review staff reports regarding compliance with this policy and Red Flag events that occurred during the reporting period.

The City Manager is responsible for reviewing reports prepared by staff regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the City Manager, to address changing identity theft risks and to

identify new or discontinued types of covered account. Any recommended material changes to the program shall be submitted to the City Manager for consideration by the Clinton City Council and Board of Trustees.

(2) The Senior level staff designated by the City Manager will report to the City Clerk at least annually, on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:

a. The effectiveness of the policies and procedures of COC in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

b. Service provider arrangements;

c. Significant incidents involving identity theft and management's responses; and

d. Recommendations for material changes to the Program.

(3) The Senior level staff designated by the City Manager is responsible for providing training to all employees responsible for or involved in opening a new covered account, restoring an existing covered account or accepting payment for a covered account with respect to the implementation and requirements of the Identity Theft Prevention Program. The City Manager shall exercise his or her discretion in determining the amount and substance of training necessary.

11. Outside Service Providers.

In the even that COC engages a service provider to perform an activity in connection with one or more covered account the City Manager shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft."

12. Treatment of Address Discrepancies.

At the present time COC is not using consumer credit reports. If in the future COC begins to use consumer credit reports, COC will comply with federal regulations regarding treatment of address discrepancies. In the event that COC receives a notice of address discrepancy, the COC employee responsible for verifying consumer addresses for the purpose of providing the municipal service or account sought by the consumer shall perform one or more of the following activities, as determined to be appropriate by such employee:

(1) Compare the information in the consumer report with:

a. Information COC obtains and uses to verify a consumer's identity in

accordance with the requirements for the Customer Information Program rules implementing 31 U.S.C. § 5318(1);

b. Information COC maintains in its own records, such as applications for service, change of address notices, other customer account records or tax records; or

c. Information COC obtains from third-party sources that are deemed reliable by the relevant COC employee; or

(2) Verify the information in the consumer report with the consumer.

13. Furnishing Consumer's Address to Consumer Reporting Agency.

(1) In the event that COC reasonably confirms that an address provided by a consumer to COC is accurate, COC is required to provide such address to the consumer reporting agency from which COC received a notice of address discrepancy with respect to such consumer. This information is required to be provided to the consumer reporting agency when:

a. COC is able to form a reasonable belief that the consumer report relates to the consumer about whom COC requested the report;

b. COC establishes a continuing relation with the consumer; and

c. COC regularly and in the ordinary course of business provides information to the consumer reporting agency from which it received the notice of address discrepancy.

(2) Such information shall be provided to the consumer reporting agency as part of the information regularly provided by the city to such agency for the reporting period in which the city establishes a relationship with the consumer.

14. Methods of Confirming Consumer Addresses.

The employee charged with confirming consumer addresses may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:

(1) Verifying the address with the consumer;
(2) Reviewing COC's records to verify the consumer's address;
(3) Verifying the address through third party sources; or
(4) Using other reasonable processes.

Report of Suspected Identity Theft

Reporting Party **Date/Time of Filing:** _____

Name _____
Account
Address: _____

City/State/Zip: _____

Billing
Address: _____

City/State/Zip: _____

Circumstances of the Suspected Identity Theft (please provide all relevant details)

_____

_____

_____

_____

Confirmation of Customer's Identity

Presentation of approved photo identification (copy attached) _____

Completed FTC Identity Theft Affidavit (copy attached) _____

Filed police report (copy attached) _____

A written police report was not taken, however a case file number was assigned _____

Case File # _____

Officer/Agent verifying the Case File # _____

I hereby acknowledge that the information I've provided is accurate and complete to the best of my knowledge.

_____ _____ _____

Customer's Printed Name Signature Date

List of Acceptable Documents

LIST A	LIST B	LIST C
Documents that Establish Both Identity and Employment Eligibility	**Documents that Establish Identity**	**Documents that Establish Employment Eligibility**
	OR	**AND**
1. U.S. Passport (unexpired or expired) **2.** Permanent Resident Card or Alien Registration Receipt Card (Form I-551) **3.** An unexpired foreign passport with a temporary I-551 stamp **4.** An unexpired Employment Authorization Document that contains a photograph (Form I-766, I-688, I-688A, I-688B) **5.** An unexpired foreign passport with an unexpired Arrival-Departure Record, Form I-94, bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, if that status authorizes the alien to work for the employer	**1.** Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address **2.** ID card issued by federal, state or local govemment agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address **3.** School ID card with a photograph **4.** Voter's registration card **5.** U.S. Military card or draft record **6.** Military dependent's ID card **7.** U.S. Coast Guard Merchant Mariner Card **8.** Native American tribal document	**1.** U.S. Social Security card issued by the Social Security Administration *(other than a card stating it is not valid for employment)* **2.** Certification of Birth Abroad issued by the Department of State *(Form FS-545 or Form DS-1350)* **3.** Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal **4.** Native American tribal document **5.** U.S. Citizen ID Card *(Form I-197)* **6.** ID Card for use of Resident Citizen in the United States *(Form I-179)* **7.** Unexpired employment authorization document issued by DHS *(other than those listed under List A)*

Red Flag Event Log

Date _____ Time _____

Red Flag Event (describe)

_____

_____

Person Reporting Event

_____

Investigating Person

_____

Immediate Actions Taken 1) _____

In Response to Event 2) _____

3) _____

4) _____

Notification of Appropriate 1) _____

Personnel (state who) 2) _____

(Include time of notification) 3) _____

Investigation Findings of

_____

Incident

_____

_____

Determination of Loss of

Customer Information _____ No Loss _____ Loss may have/did occur

Mitigating Action(s) Taken 1) _____

2) _____

3) _____

As required, Actions taken 1) _____

To notify Affected Customers 2) _____

3) _____

Proposed Changes to Processes, Procedures, Policies to Limit Potential of Loss.

_____

_____

_____

_____

_____

_____

_____ _____

Investigating Person Signature

Date