

RESOLUTION NO. 2009-10

**A RESOLUTION OF THE TOWN COUNCIL OF THE TOWN OF SILVER CITY
TO ADOPT AN "IDENTITY THEFT PREVENTION PROGRAM"**

Sponsored by Mayor James R. Marshall

WHEREAS, pursuant to regulations promulgated by the United States Federal Trade Commission ("FTC"), commonly referenced as the "Red Flag Rules", all persons or entities coming within the definition of "creditor" as prescribed by the aforementioned regulations must adopt and implement an Identity Theft Prevention Program, which identifies specific policies and practices designed to detect, prevent and mitigate identity theft; and

WHEREAS, the Town of Silver City is a "creditor" within the meaning of the FTC regulations by virtue of it being a provider of services prior to payment, such as is the case regarding the delivery of water, sewer, and garbage services; and

WHEREAS, the FTC mandates that the governing body of all municipalities must adopt an "Identity Theft Prevention Program" and implement such program in compliance therewith prior to May 1, 2009;

BE IT RESOLVED, THEREFORE, THAT:

The Town Council of the Town of Silver City hereby adopts the "Identity Theft Prevention Program" memorialized by the attached written document (Appendix "A"), to be effective on May 1, 2009, and designates the Town Manager to be the administrator thereof.

PASSED, ADOPTED and APPROVED this 28th day of April, 2009.

/s/
James R. Marshall, Mayor

Attest:

/s/
Yolanda C. Holguin, Acting Town Clerk

TOWN OF SILVER CITY

IDENTITY THEFT PREVENTION PROGRAM (“ITPP”)

INTRODUCTION

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. The Town of Silver City (“TSC”) 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 (ITPP), which will use red flags to detect, prevent and mitigate identity theft related to information used in covered accounts. The TSC 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. The TSC residential/commercial 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 primarily for household purposes and allowing for multiple payments or transactions.

IDENTITY THEFT PREVENTION PROGRAM

1. Purpose.

The purpose of this Program is to comply with 16 CFR § 681.2 in order to attempt 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 help prevent identity theft.

2. Definitions.

For the purposes of this Program, the definitions found in Appendix A shall apply.

3. Findings.

- 1) The TSC is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.
- 2) Covered accounts offered to customers for the provision of TSC services include residential water, sewer and sanitation accounts.
- 3) The TSC 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, and making payments on such accounts have been identified as potential processes in which identity theft could occur.
- 5) The TSC limits access to personal identifying information to those employees in the Finance department 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 (sample included as Appendix B) associated with the covered accounts are maintained in the Utility Billing locked vault. Information provided in the application is entered directly into the TSC's computer system and is accessible only to those employees in the Finance department and to the TSC's Information Technician.
- 6) The TSC 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 the TSC and the customer during the customer's application for service process.

PROCEDURES

4. Process of Establishing a Covered Account.

- A. As a precondition to opening a covered account in the TSC, each applicant shall provide the TSC with personal identifying information of the customer, which shall be in the form of a valid state or federal government issued identification card, such as a state issued driver's license, a state issued identification card, a U.S. government issued passport or visa, or a U.S. military identification card, all of which must contain a photograph of the customer. 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.

- B. Each account shall be assigned an account number, which the computer software does.
- C. An applicant's personal identifying information shall be entered directly into the TSC's computer system and all written applications shall be placed in the Utility Billing vault.
- D. TSC 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. Applications that are allowed to be faxed in or mailed in for the convenience of the customer, are required to have a notary public attest to the individual's personal identifying information.
- E. The TSC does not now allow customers to pay billing statements online. Should the TSC begin allowing online payments, additional precautions will be put in place to address the issue at that time.

5. Access to Covered Account Information.

- A. Access to customer accounts shall be password protected and shall be limited to authorized TSC Finance personnel.
- B. Passwords shall be changed by the TSC Information Technician at the direction of the Deputy Finance Director, as deemed necessary.
- C. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Deputy Finance Director and the password shall be changed immediately.
- D. Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Utility Billing Supervisor, Deputy Finance Director, and/or Town Manager, and if the situation warrants, the Town Attorney.

6. Credit Card Payments.

- A. At the present time, the TSC does not allow payments through the Internet. If in the future such payments are allowed, appropriate guidelines will be put into place to certify that an adequate identity theft prevention program is in place that is applicable to such payments.
- B. All credit card payments made over the telephone shall be entered directly into the TSC's

bank credit card terminal for approval. The customer will be required to verify personal identifying information to be able to make such a payment. Associated paperwork generated by the terminal will be kept with all daily balancing reconciliation information and be stored in the Deputy Finance Director's office, which is locked on a daily basis.

- C. Customer bank draft account information will be entered into the computer software database and the bank draft site, which are both protected and accessed by password. Associated paperwork generated by this process will be stored in either the Utility Billing Vault or the Deputy Finance Director's office, which are both locked on a daily basis.
- D. If a third party's credit card is to be used to pay the account of a customer, the third party must present in person his/her credit card and the customer's bill for payment. They must also 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:

- A. *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:
 - 1) A fraud or active duty alert that is included with a consumer report;
 - 2) A notice of credit freeze in response to a request for a consumer report;
 - 3) A notice of address discrepancy provided by a consumer reporting agency;
 - 4) 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:
 - 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. *Suspicious documents.* Examples of suspicious documents include:
 - 1) Documents provided for identification that appear to be altered or forged;
 - 2) Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
 - 3) Identification on which the information is inconsistent with the information provided by the applicant or customer;
 - 4) Identification on which the information is inconsistent with readily accessible information that is on file with the TSC;
 - 5) An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

- C. *Suspicious personal identification, such as suspicious address change.* Examples of suspicious identifying information include:
- 1) Personal identifying information that is inconsistent with external information sources used by the TSC. For example:
 - a. The address does not match any address in the consumer report (if used by the TSC); or
 - b. The social security number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File (if used by the TSC).
 - 2) 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.
 - 3) 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 the TSC.
 - 4) 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.
 - 5) The social security number provided is the same as that submitted by other applicants or 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 applicants or customers.
 - 7) 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
 - 8) Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.
 - 9) The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- D. *Unusual use of or suspicious activity relating to a covered account.* Examples of suspicious activity include:
- 1) An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - a. Nonpayment when there is no history of late or missed payments;
 - b. A material change in the water usage.
 - 2) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
 - 3) The TSC is notified that the customer is not receiving paper account billings.
 - 4) The TSC is notified of unauthorized charges or transactions in connection with a customer's account.
 - 5) The TSC is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.
- E. *Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or publishing relating to covered accounts.*

8. Prevention and Mitigation of Identity Theft.

- A. Restoring an Existing Covered Account or Accepting Payment: In the event that any TSC 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 Deputy Finance Director or relevant designee. If the employee at his or her own discretion deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall also convey this information to the Deputy Finance Director or relevant designee, who may at his or her own discretion determine that no further action is necessary. If the Deputy Finance Director, at his or her own discretion determines that further action is necessary, a TSC employee shall perform one or more of the following responses, as determined to be appropriate by the Deputy Finance Director:
- 1) Contact the customer;
 - 2) 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:
 - a. Change any account numbers, passwords, security codes, or other security devices that permit access to an account; or
 - b. Close the account;
 - 3) 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;
 - 4) Notify a debt collector within three (3) 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's 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;
 - 5) 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
 - 6) Take other appropriate action to prevent or mitigate identity theft.
- B. Opening a New Covered Account: In the event that any TSC employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect to an application for a new account, such employee shall use his or her discretion to determine whether such red flags or combination of red flags suggests that identity theft or attempted identity theft is likely or probable. 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

Deputy Finance Director or relevant designee. 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 also convey this information to the Deputy Finance Director or relevant designee, who may, in his or her discretion, determine that no further action is necessary. If the Deputy Finance Director, in his or her discretion, determines that further action is necessary, an appointed TSC employee shall perform one or more of the following responses, as determined to be appropriate by the Deputy Finance Director:

- 1) Request additional identifying information from the applicant;
- 2) Deny the application for the new account;
- 3) Notify law enforcement of possible identity theft; or
- 4) Take other appropriate action to prevent or mitigate identity theft.

9. Updating the Program.

Upon the recommendation of the Town Manager, the Town Council shall annually review and, as deemed necessary by the Town Council, update the Identity Theft Prevention Program (ITPP) along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the TSC and its covered accounts from identity theft. In doing so, the Town Council shall consider the following factors and exercise its discretion in amending the program:

- 1) The TSC'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 the TSC offers or maintains; and
- 5) Updates in service provider arrangements.

10. Program Administration.

- A. In accordance with specified guidelines, the TSC governing body has designated an Oversight Committee composed of the Deputy Finance Director, the Utility Billing Supervisor, and the Town Clerk to ensure the Program's regulatory compliance. The Oversight Committee is responsible for, but not limited to:
 - 1) The development and implementation of the Program.
 - 2) Ensuring compliance with all Program requirements as stated in this policy;
 - 3) 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).
 - 4) At least annually, review staff reports regarding compliance with this policy and Red Flag events that occurred during the reporting period.
 - 5) At least annually, address and agree on any changes that may need to be made to the Program and submit these annually to the Town Manager for consideration.
- B. The Deputy Finance Director is responsible for reviewing reports prepared by staff (prepared at least bi-annually) regarding compliance with red flag requirements and with recommending material changes to the Program, as necessary in the opinion of the Deputy Finance Director, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the Program shall be submitted by the Deputy Finance Director to the Oversight Committee

for review and consensus. Final recommendations coming from the Oversight Committee will then be forwarded to the Town Manager for consideration annually. The Town Manager is responsible for reviewing these reports and recommendations prepared by the Deputy Finance Director and Oversight Committee and address any recommended material changes to the Program to the Town Council for consideration.

- 1) The Senior Level Staff designated by the Deputy Finance Director will report to the Deputy Finance Director at least semi-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 the TSC 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;
 - d. Recommendations for material changes to the Program up for review annually.
- C. The Senior Level Staff designated by the Deputy Finance Director is responsible for providing training to all Town Utilities Department staff, other relevant Town staff, and third-party service providers 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 ITPP. They are to receive effective oversight to ensure that the activity is conducted in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. The Deputy Finance Director shall exercise his or her discretion in determining the amount and substance of training necessary.

11. Outside Service Providers.

In the event that the TSC engages a service provider to perform an activity in connection with one or more covered accounts, the Deputy Finance Director 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. The Deputy Finance Director may warrant the assistance of the Oversight Committee, the assigned Senior Level Staff, the Town Manager, or the Town Attorney for any questions that may arise.

12. Treatment of Address Discrepancies.

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

- A. Compare the information in the consumer report with:
 - 1) Information the TSC obtains and uses to verify a customer's identity in accordance with the requirements for the Customer Information Program rules implementing 31 U.S.C. § 5318(1);
 - 2) Information the TSC maintains in its own records, such as applications for service, change of address notices, other customer account records or tax records; or
 - 3) Information the TSC obtains from third-party sources that are deemed reliable by the relevant TSC employee; or
- B. Verify the information in the consumer report/customer account with the customer.

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

- A. In the event that the TSC reasonably confirms that an address provided by a consumer to the TSC is accurate, the TSC is required to provide such address to the consumer reporting agency from which the TSC received a notice of address discrepancy with respect to such consumer. This information is required to be provided to the consumer reporting agency when:
 - 1) The TSC is able to form a reasonable belief that the consumer report relates to the consumer about whom the TSC requested the report;
 - 2) The TSC establishes a continuing relation with the consumer; and
 - 3) The TSC regularly, and in the ordinary course of business, provides information to the consumer reporting agency from which it received the notice of address discrepancy.
- B. Such information shall be provided to the consumer reporting agency as part of the information regularly provided by the TSC to such agency for the reporting period in which the TSC establishes a relationship with the consumer.

14. Methods of Confirming Consumer Addresses.

The TSC 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 the TSC's records to verify the consumer's address;
- 3) Verifying the address through third party sources; or
- 4) Using other reasonable processes.

APPENDIX A

- A. "TSC" means the Town of Silver City.
- B. "Covered Account" means (1) 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 or Municipal Court imposed fine or cost**, checking account, or savings account; (2) Any other account that the financial institution or creditor offers or maintains for 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 or 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 the TSC 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 electronic identification number, address or routing code; or
 - 3) 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. "Oversight Committee" means the Committee appointed by the TSC to oversee operation and compliance of the TSC's ITPP in accordance with the requirements of the Fair and Accurate Credit Transaction Act.
- K. "Personal Identifying Information" means a person's credit card account information, debit card account information, bank account information, and driver's license information; and for a natural person includes their social security number, mother's birth name, and date of birth.
- L. "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
- M. "Service provider" means a person that provides a service directly to the TSC.

APPENDIX B
(Customer Application)

TOWN OF SILVER CITY
APPLICATION FOR UTILITY SERVICES

PO BOX 1188
505-538-3731

SILVER CITY, NM 88062
505-538-5123(FAX)

PLEASE PRINT Deposit _____

ACCT. NUMBER _____ TURN ON DATE _____

NAME _____ DATE _____

SERVICE ADDRESS _____

MAILING ADDRESS _____

ARE YOU RENTING? Y OR N IF YES, FROM WHOM? _____

EMPLOYER _____ EMPLOYER PHONE# _____

HOME PHONE# _____ SSN _____ DL# _____

DOB _____ SPOUSE NAME _____

NAME & ADDRESS OF NEAREST RELATIVE _____

**PLEASE READ IMPORTANT INFO ON HANDLING OF
DEPOSIT BEFORE SIGNING!!!**

ORDINANCE NO. 1049
SECTION 30-41(A) THE WATER SERVICE DEPOSIT SHALL BE REFUNDED TO THE PROPERTY OWNER ONE YEAR AFTER FIRST BILLING UPON COMMENCEMENT OF WATER SERVICE IF THE PROPERTY OWNER HAS A SATISFACTORY CREDIT RATING AS DEFINED IN THE TOWN'S UTILITY DEPOSIT POLICY. THE WATER SERVICE DEPOSIT SHALL BE REFUNDED TO THE CUSTOMER, IF IDENTIFIED AS OTHER THAN THE PROPERTY OWNER (RENTEE, LESSEE, ETC.), ONLY UPON FINAL TERMINATION OF SERVICE WITH THE TOWN AND IN ACCORDANCE WITH THE TOWN'S UTILITY DEPOSIT POLICY, AND ONLY IN ACCORDANCE WITH THE PROVISION OF SECTION 30-42.

COPIES OF ORDINANCE ARE AVAILABLE UPON REQUEST FOR VIEWING ONLY

IF YOUR BILL DUE DATE LANDS ON A WEEKEND OR A HOLIDAY PLEASE MAKE SURE TO PAY BEFORE THIS DATE

NOTE: Payments received after 2:30pm ARE CREDITED to the next day's business.

SIGNATURE _____

**APPENDIX C
(FORMS)**

Report of Suspected Identity Theft

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

Customer 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, but a case file number was assigned _____

Case File # _____

Officer/Agent verifying the Case File # _____

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

Customer's Printed Name

Signature

Date

Red Flag Event Log

Date _____ Time _____

Red Flag Event (describe): _____

Person Reporting Event: _____

Investigating Person: _____

Immediate Actions Taken in Response to Event:

1) _____

2) _____

3) _____

4) _____

Notification of Appropriate Personnel (state who and time of notification):

1) _____

2) _____

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 to Notify Affected Customers:

- 1) _____
- 2) _____
- 3) _____

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

Investigating Person

Signature

Date

Identity Theft Prevention Program Semi-Annual Review and Annual Report

Date	Responsible Person	
_____	_____	On or about 1 May 2009, Key Personnel will conduct a semi-annual review of the program. Review will cover, as a minimum,
		_____ Review and discussion regarding all Red Flag events that occurred during the previous six months, whether a loss of information occurred or not. Discussion will include identifying the particular event, immediate actions taken and actions taken to limit customer exposure or preventative measures for future events.
		_____ Review and discussion of current processes and procedures to determine if changes should be considered.
		_____ Upon staff review and developed action, written review material will be maintained and secured in accordance with established policy.
_____	_____	On or about 1 November 2009, Key Personnel will conduct a semi-annual review of the program. Review will cover, as a minimum,
		_____ Review and discussion regarding all Red Flag events that occurred during the previous six months, whether a loss of information occurred or not. Discussion will include identifying the particular event, immediate actions taken and actions taken to limit customer exposure or preventative measures for future events.
		_____ Review and discussion of current processes and procedures to determine if changes should be considered.
		_____ Upon staff review and developed action, written review material will be maintained and secured in accordance with established policy.
_____	_____	Within three days of the 1 November 2009 review, a written report will be submitted to the Governing Body, or the Oversight Committee as designated by the Governing Body. The report will summarize the Red Flag events that have occurred during the previous 12 month period, the actions taken, changes that have occurred within the program and/or recommendations of changes to the Program should such actions require Governing Body approval.